ALIBABA CLOUD

Alibaba Cloud

Security Center

Precautions

Document Version: 20220704

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ Danger: Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
🔈 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	🔈 Notice: If the weight is set to 0, the server no longer receives new requests.
? Note	A note indicates supplemental instructions, best practices, tips, and other content.	? Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Vulnerabilities

1.1. Overview

This topic provides an overview of the vulnerability fixing feature of Security Center. You can use Security Center to detect and fix common vulnerabilities with a few clicks. You can enable Security Center to automatically scan servers for vulnerabilities on a regular basis. You can also manually perform quick scan tasks to scan servers for vulnerabilities. You can view the overall security status of your assets. If vulnerabilities are detected, you can use the vulnerability fixing feature to fix the vulnerabilities.

Context

When you fix a Linux software vulnerability in the Security Center console with a few clicks, the YUM utility of Linux automatically downloads, installs, and deletes the patch that is required to fix the vulnerability. The YUM utility of Linux deletes the patch three days after the vulnerability is fixed. No manual operations are required.

When you fix a Windows system vulnerability in the Security Center console with a few clicks, the Security Center agent automatically downloads, installs, and deletes the patch that is required to fix the vulnerability. No manual operations are required. If the Security Center agent does not delete the patch three days after the vulnerability is fixed, you can manually delete the patch package. For more information, see How do I delete the patch that is required to fix a Windows system vulnerability from the directory of the Security Center agent?

Limits

The following symbols are used in the table:

- √: indicates that the feature is supported.
- ×: indicates that the feature is not supported.

Vulnerability type	Feature	Basic edition	Anti-virus edition	Advanced edition	Enterprise edition	Ultimate edition
Linux software vulnerability	Vulnerability detection	√	√	√	√	√
	Vulnerability fixing	×	×	√	√	√
Windows system vulnerability	Vulnerability detection	√	√	√	√	√
	Vulnerability fixing	×	×	√	√	√
Web-CMS vulnerability	Vulnerability detection	√	√	√	√	√
	Vulnerability fixing	×	×	√	√	√

Vulnerability type	Feature	Basic edition	Anti-virus edition	Advanced edition	Enterprise edition	Ultimate edition
Urgent vulnerability	Vulnerability detection	√	√	√	√	√
	Vulnerability fixing	×	×	×	×	×
Application vulnerability	Vulnerability detection	×	×	×	√	√
	Vulnerability fixing	×	×	×	×	×

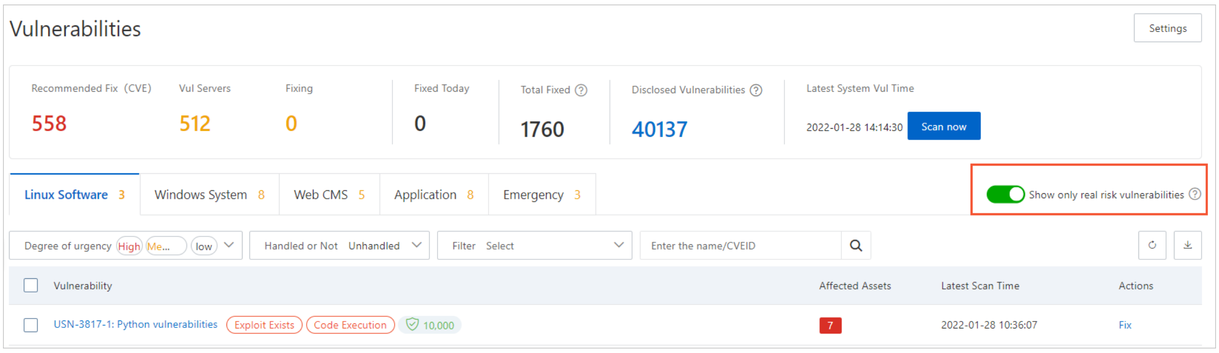
Note Security Center can detect urgent vulnerabilities and application vulnerabilities, but cannot fix these types of vulnerabilities. If you want to fix these types of vulnerabilities, you must log on to the server on which the vulnerabilities are detected and manually fix the vulnerabilities based on the fix suggestions that are provided on the details pages of the vulnerabilities.

Supported operating systems of vulnerability detection and vulnerability fixing

Operating system	Version
CentOS	CentOS 5, CentOS 6, CentOS 7, and CentOS 8. For CentOS 5, CentOS 6, and CentOS 8, Security Center can detect and fix only the vulnerabilities that are disclosed before their respective end of life (EOL) date.
Redhat	Redhat 5, Redhat 6, Redhat 7, and Redhat 8. For Redhat 5 and Redhat 6, Security Center can detect and fix only the vulnerabilities that are disclosed before their respective EOL date.
Ubuntu	Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, Ubuntu 20, and Ubuntu 21. For Ubuntu 12, Ubuntu 14, and Ubuntu 16, Security Center can detect and fix only the vulnerabilities that are disclosed before their respective EOL date.
Windows Server	Windows Server 2008, Windows Server 2012, Windows Server 2016, and Windows Server 2019. For Windows Server 2008, Security Center can detect and fix only the vulnerabilities that are disclosed before the EOL date.
Alibaba Cloud Linux	Alibaba Cloud Linux 2.1903 and Alibaba Cloud Linux 3.
Anolis OS	Anolis OS 7.9 and Anolis OS 8.

Easily exploitable vulnerabilities

The **Show only real risk vulnerabilities** switch is added to the upper-right corner of the vulnerability list on the Vulnerabilities page. After you turn on the switch, Security Center displays only the vulnerabilities whose urgency score is high in the vulnerability list. After you turn off the switch, Security Center displays all vulnerabilities in the vulnerability list.



Recommended Fix (CVE) 558
Vul Servers 512
Fixing 0
Fixed Today 0
Total Fixed 1760
Disclosed Vulnerabilities 40137
Latest System Vul Time 2022-01-28 14:14:30

Linux Software 3 | Windows System 8 | Web CMS 5 | Application 8 | Emergency 3

Degree of urgency High Me... low | Handled or Not Unhandled | Filter Select | Enter the name/CVEID

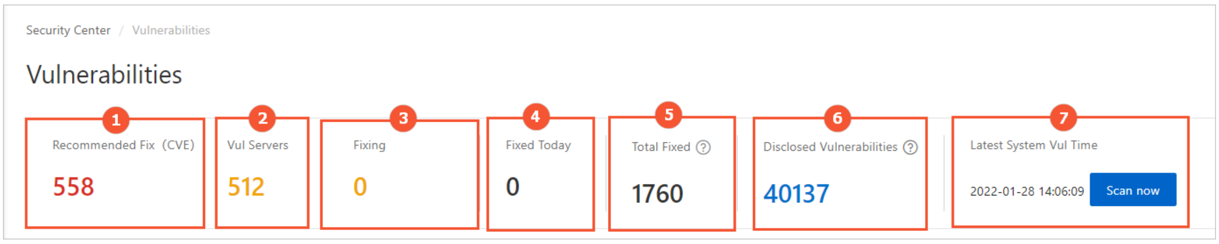
Vulnerability	Affected Assets	Latest Scan Time	Actions
□ USN-3817-1: Python vulnerabilities Exploit Exists Code Execution 10,000	7	2022-01-28 10:36:07	Fix

After you turn on the switch, Security Center automatically analyzes vulnerabilities on your system, and detects and displays easily exploitable vulnerabilities. In addition, the Vulnerabilities page displays only vulnerabilities whose urgency score is greater than or equal to 13.5. If you want to view only vulnerabilities whose urgency score is high, we recommend that you turn on the switch.

> **Note** The urgency score of a vulnerability helps you determine whether to immediately fix the vulnerability. If the urgency score of a vulnerability is greater than or equal to 13.5, the vulnerability is critical and must be immediately fixed. For more information, see Priorities to fix vulnerabilities.

Vulnerability statistics

You can log on to the Security Center console and view vulnerability statistics in the upper part of the **Vulnerabilities** page.

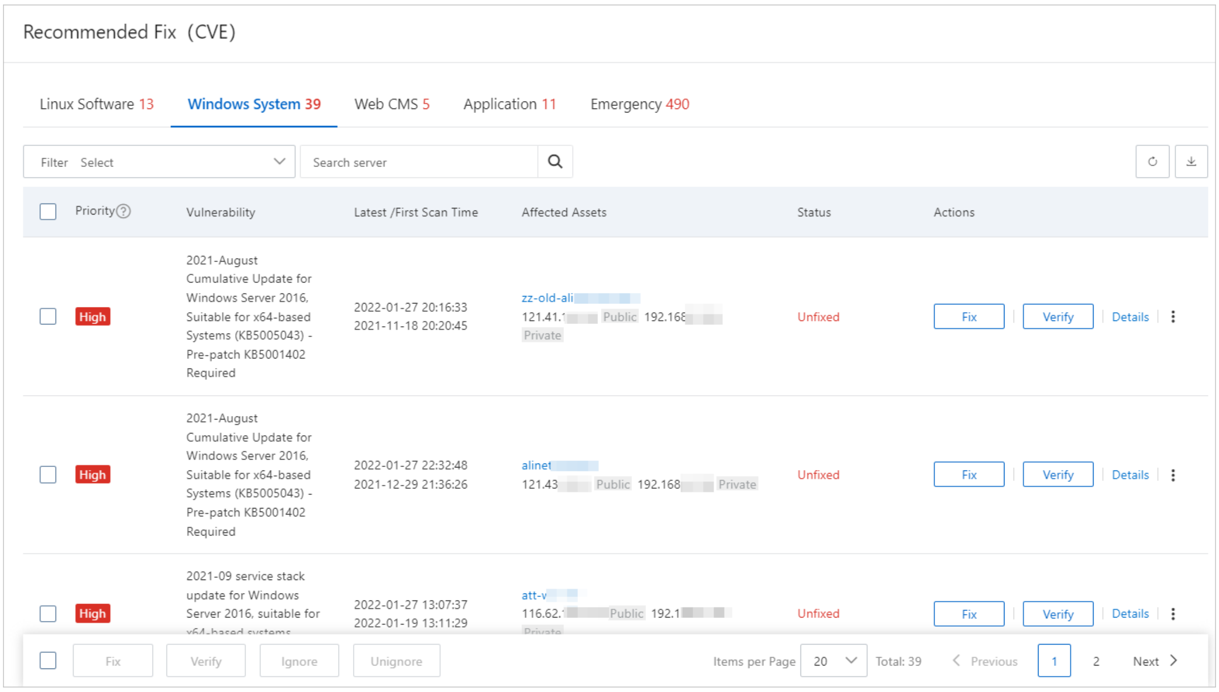


Recommended Fix (CVE) 558
Vul Servers 512
Fixing 0
Fixed Today 0
Total Fixed 1760
Disclosed Vulnerabilities 40137
Latest System Vul Time 2022-01-28 14:06:09

- Recommended Fix (CVE) (marked 1 in the preceding figure)
- Vul Servers (marked 2 in the preceding figure)
- Fixing (marked 3 in the preceding figure)
- Fixed Today (marked 4 in the preceding figure)
- Total Fixed (marked 5 in the preceding figure)
- Disclosed Vulnerabilities (marked 6 in the preceding figure)
- Latest System Vul Time (marked 7 in the preceding figure)

Recommended Fix (CVE)

Click the number below **Recommended Fix (CVE)** to go to the **Recommended Fix (CVE)** panel. In the panel, you can view all types of vulnerabilities with the high priority. For more information about how to fix vulnerabilities, see View and handle Linux software vulnerabilities, View and handle Windows system vulnerabilities, View and handle Web-CMS vulnerabilities, View and handle application vulnerabilities, and View and handle urgent vulnerabilities.



Recommended Fix (CVE)

Linux Software 13 | Windows System 39 | Web CMS 5 | Application 11 | Emergency 490

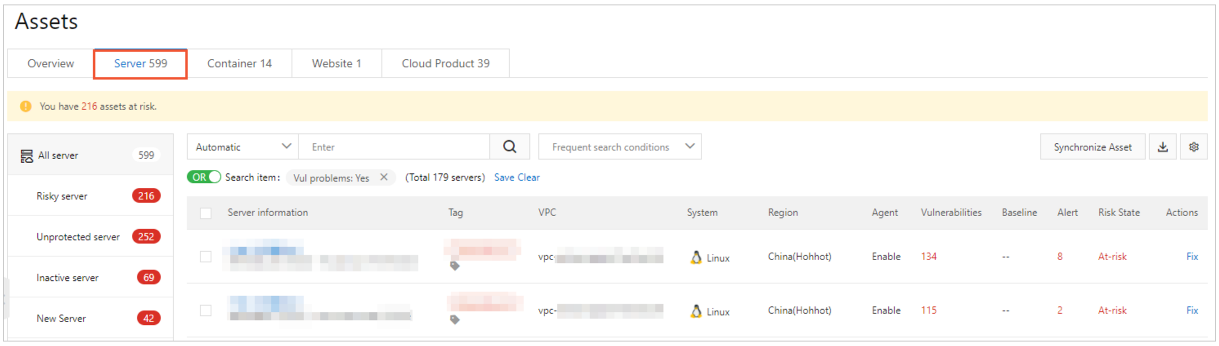
Filter Select | Search server

□	Priority	Vulnerability	Latest /First Scan Time	Affected Assets	Status	Actions
□	High	2021-August Cumulative Update for Windows Server 2016, Suitable for x64-based Systems (KB5005043) - Pre-patch KB5001402 Required	2022-01-27 20:16:33 2021-11-18 20:20:45	zz-old-ali[redacted] 121.41.1[redacted] Public 192.168[redacted] Private	Unfixed	Fix Verify Details ⋮
□	High	2021-August Cumulative Update for Windows Server 2016, Suitable for x64-based Systems (KB5005043) - Pre-patch KB5001402 Required	2022-01-27 22:32:48 2021-12-29 21:36:26	alinet[redacted] 121.43[redacted] Public 192.168[redacted] Private	Unfixed	Fix Verify Details ⋮
□	High	2021-09 service stack update for Windows Server 2016, suitable for x64-based systems	2022-01-27 13:07:37 2022-01-19 13:11:29	att-v[redacted] 116.62.[redacted] Public 192.1[redacted] Private	Unfixed	Fix Verify Details ⋮

□ Fix Verify Ignore Unignore | Items per Page 20 | Total: 39 | < Previous 1 2 Next >

Vul Servers

Click the number below **Vul Servers** to go to the **Server(s)** tab of the **Assets** page. On the Server(s) tab, you can view the details about the servers on which vulnerabilities are detected.



Assets

Overview | Server 599 | Container 14 | Website 1 | Cloud Product 39

You have 216 assets at risk.

All server	599
Risky server	216
Unprotected server	252
Inactive server	69
New Server	42

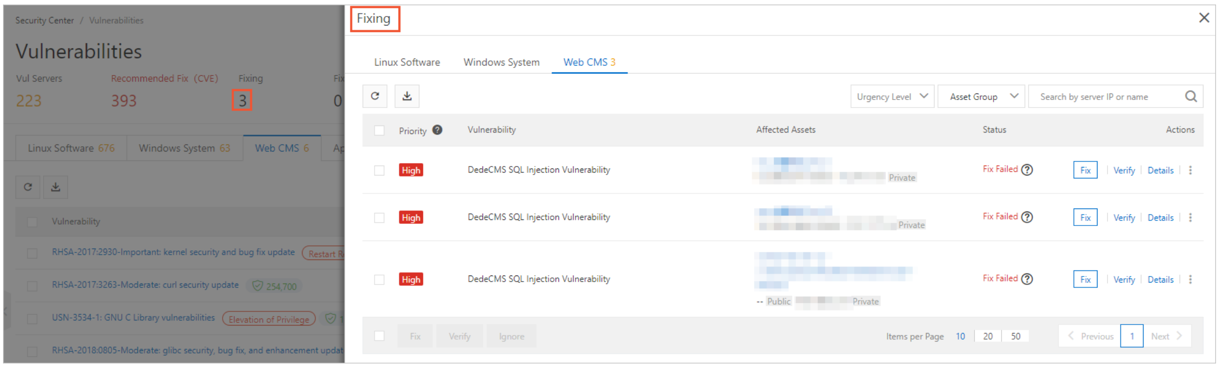
Automatic | Enter | Frequent search conditions | Synchronize Asset

OR Search item : Vul problems: Yes ✕ (Total 179 servers) Save Clear

□	Server information	Tag	VPC	System	Region	Agent	Vulnerabilities	Baseline	Alert	Risk State	Actions
□	[redacted]	[redacted]	vpc-[redacted]	Linux	China(Hohhot)	Enable	134	--	8	At-risk	Fix
□	[redacted]	[redacted]	vpc-[redacted]	Linux	China(Hohhot)	Enable	115	--	2	At-risk	Fix

Fixing

Click the number below **Fixing** to go to the **Fixing** panel. In the panel, you can view the list of vulnerabilities that are being fixed and the fix progress.



Security Center / Vulnerabilities

Vulnerabilities

Vul Servers 223 | Recommended Fix (CVE) 393 | Fixing 3 | Fix 0

Linux Software 676 | Windows System 63 | Web CMS 6 | Ap

	Vulnerability
□	RHSA-2017:2930-Important: kernel security and bug fix update (Restart R
□	RHSA-2017:3263-Moderate: curl security update 254,700
□	USN-3534-1: GNU C Library vulnerabilities (Elevation of Privilege)
□	RHSA-2018:0805-Moderate: glibc security, bug fix, and enhancement updat

Fixing

Linux Software | Windows System | Web CMS 3

Urgency Level | Asset Group | Search by server IP or name

□	Priority	Vulnerability	Affected Assets	Status	Actions
□	High	DedeCMS SQL Injection Vulnerability	[redacted] Private	Fix Failed	Fix | Verify | Details
□	High	DedeCMS SQL Injection Vulnerability	[redacted] Private	Fix Failed	Fix | Verify | Details
□	High	DedeCMS SQL Injection Vulnerability	[redacted] -- Public [redacted] Private	Fix Failed	Fix | Verify | Details

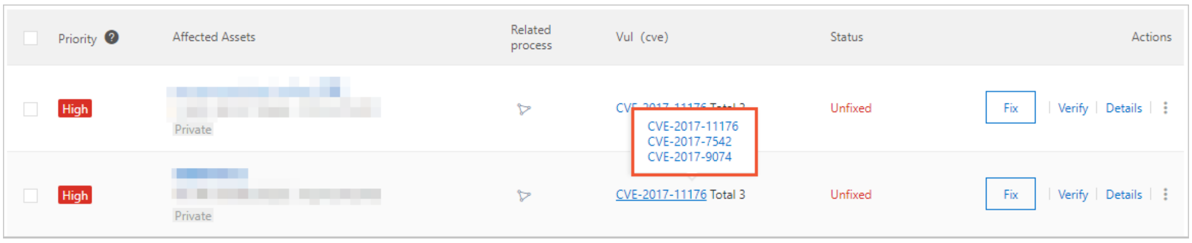
□ Fix Verify Ignore Items per Page 10 20 50 < Previous 1 Next >

Fixed Today

Click the number below **Fixed Today** to go to the **Fixed Today** panel. In the Fixed Today panel, you can view information about the assets affected by the vulnerabilities that are fixed on the current day.

You can perform the following operations in the panel:

- **View related processes**: Click the icon in the **Related process** column to view the processes or service systems that may be affected when Security Center fixes the vulnerability.
- **View the details about the Alibaba Cloud vulnerability library**: Click a CVE ID in the **Vul (cve)** column to view details about the vulnerability in the Alibaba Cloud vulnerability library.
  If multiple vulnerabilities are detected on an asset, the number of vulnerabilities is displayed in the **Vul (cve)** column. If you want to view the details about a vulnerability, move the pointer over the displayed CVE ID and click the CVE ID.



□	Priority	Affected Assets	Related process	Vul (cve)	Status	Actions
□	High	[redacted] Private		CVE-2017-11176 Total 3 CVE-2017-11176 CVE-2017-7542 CVE-2017-9074	Unfixed	Fix | Verify | Details
□	High	[redacted] Private		CVE-2017-11176 Total 3	Unfixed	Fix | Verify | Details

- **View the details about a vulnerability fix**: Click **Details** in the **Actions** column to view the descriptions and risks of the vulnerability fix.
- **Undo a vulnerability fix**: If you have created a snapshot for an asset, you can undo the fixes of vulnerabilities on the asset. To undo a fix, click **Undo Fix** in the **Actions** column, select the snapshot that you have created, and then click **OK**.

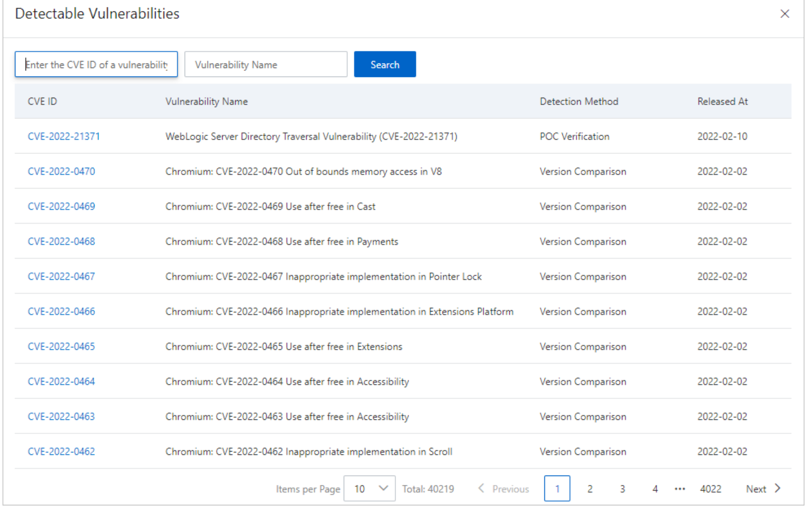
> **Note** The snapshot of an asset allows you to undo the fixes of the Linux software vulnerabilities and Windows system vulnerabilities that are detected on the asset.

Total Fixed

Click the number below **Total Fixed** to go to the **Total Fixed** panel. In the Total Fixed panel, you can view information about the assets affected by vulnerabilities that are fixed.

Disclosed Vulnerabilities

Click the number below **Disclosed Vulnerabilities** to go to the **Detectable Vulnerabilities** panel. In the Detectable Vulnerabilities panel, you can view the list of and details about the vulnerabilities that can be detected by Security Center. The details include CVE IDs, vulnerability names, vulnerability detection methods, and vulnerability disclosure time. In the panel, you can also enter a CVE ID or vulnerability name above the vulnerability list to search for a specific vulnerability. This way, you can check whether the vulnerability can be detected by Security Center. You can click the CVE ID of a vulnerability to view details about the vulnerability in the Alibaba Cloud vulnerability library.


Detectable Vulnerabilities
×
Enter the CVE ID of a vulnerabilit
Vulnerability Name
Search

CVE ID	Vulnerability Name	Detection Method	Released At
CVE-2022-21371	WebLogic Server Directory Traversal Vulnerability (CVE-2022-21371)	POC Verification	2022-02-10
CVE-2022-0470	Chromium: CVE-2022-0470 Out of bounds memory access in V8	Version Comparison	2022-02-02
CVE-2022-0469	Chromium: CVE-2022-0469 Use after free in Cast	Version Comparison	2022-02-02
CVE-2022-0468	Chromium: CVE-2022-0468 Use after free in Payments	Version Comparison	2022-02-02
CVE-2022-0467	Chromium: CVE-2022-0467 Inappropriate implementation in Pointer Lock	Version Comparison	2022-02-02
CVE-2022-0466	Chromium: CVE-2022-0466 Inappropriate implementation in Extensions Platform	Version Comparison	2022-02-02
CVE-2022-0465	Chromium: CVE-2022-0465 Use after free in Extensions	Version Comparison	2022-02-02
CVE-2022-0464	Chromium: CVE-2022-0464 Use after free in Accessibility	Version Comparison	2022-02-02
CVE-2022-0463	Chromium: CVE-2022-0463 Use after free in Accessibility	Version Comparison	2022-02-02
CVE-2022-0462	Chromium: CVE-2022-0462 Inappropriate implementation in Scroll	Version Comparison	2022-02-02

Items per Page 10 Total: 40219 < Previous 1 2 3 4 ••• 4022 Next >

Latest System Vul Time

View the time when a vulnerability scan task was last performed below Latest System Vul Time.

> **Note** If you want to manually scan newly purchased Elastic Compute Service (ECS) instances at an unscheduled time, click **Scan now** to start the scan task. For more information, see Use the quick scan feature.

1.2. Use the quick scan feature

Security Center supports automatic periodic scan tasks and manual scan tasks. This topic describes how to run a manual scan task.

Context

If you want to run a scan task on a server at an unscheduled point in time, you can click **Scan now** in the Security Center console to start a manual scan task.
For more information about the intervals at which automatic tasks scan for different types of vulnerabilities, see Vulnerability detection cycle.

You can configure an automatic periodic scan task. For more information, see Configure vulnerability settings.

Limits

The following table describes the check items that are supported by each edition of Security Center.

Note The following symbols are used in the table:

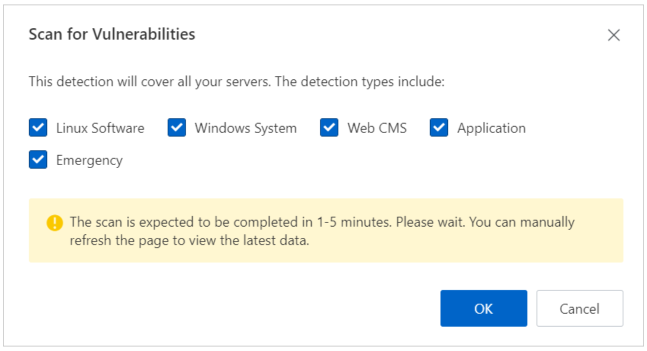
- ×: This edition does not support this check item.
- √: This edition supports this check item.
- ○: The Basic and Anti-virus editions of Security Center support only the automatic detection of vulnerabilities. These editions do not support quick scan for vulnerabilities or fixing of vulnerabilities. Before you can use Security Center to run manual scan tasks, you must upgrade Security Center to the Advanced, Enterprise, or Ultimate edition. If you want to use Security Center to fix detected vulnerabilities, you must upgrade Security Center to the Advanced, Enterprise, or Ultimate edition.

Vulnerabilities					
Linux software vulnerabilities	○	○	√	√	√
Windows system vulnerabilities	○	○	√	√	√
Web-CMS vulnerabilities	○	○	√	√	√
Application vulnerabilities	×	×	×	√	√
Urgent vulnerabilities	√	√	√	√	√

Procedure

1.
2.
3. On the **Vulnerabilities** page, click **Scan now**.

   Before you click **Scan now**, click **Settings** in the upper-right corner of the page. In the **Settings** panel, click **Manage** to the right of each check item and check whether the servers that you want to scan are displayed in the Assets section.
4. In the **Scan for vulnerabilities** dialog box, select the type of vulnerabilities that you want to scan for and click **OK**.



Scan for Vulnerabilities

This detection will cover all your servers. The detection types include:

☑ Linux Software ☑ Windows System ☑ Web CMS ☑ Application
☑ Emergency

The scan is expected to be completed in 1-5 minutes. Please wait. You can manually refresh the page to view the latest data.

> ⓘ **Note** After you click **Scan now**, Security Center scans all protected assets. The time required to complete the scan is approximately 30 minutes. Wait until the scan is complete. You can refresh the page to view the most recent statistics.

After the scan is complete, you can click a tab on the Vulnerabilities page to view the most recent scan results. For more information about vulnerability scan results, see Vulnerability statistics.

1.3. View and handle Linux software vulnerabilities

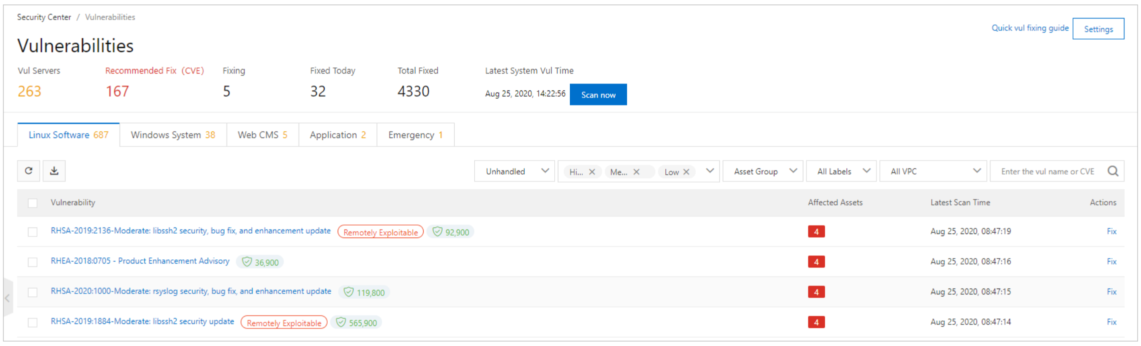
Security Center can detect Linux software vulnerabilities and allows you to fix the vulnerabilities with a few clicks. This topic describes how to view and handle Linux software vulnerabilities.

Limits

The and editions of Security Center detect but do not fix vulnerabilities. To use Security Center to fix vulnerabilities with a few clicks, you must purchase the , , or edition. For more information about the features supported by different Security Center editions, see Features.

View the basic information about a vulnerability

1.
2.
3. On the **Vulnerabilities** page, click the **Linux Software** tab.
4. On the **Linux Software** tab, view the Linux software vulnerabilities that are detected by Security Center. In most cases, the name of a Linux software vulnerability starts with *USN*, *RHSA*, or *CVE*.
    - **View vulnerabilities**



Vulnerabilities

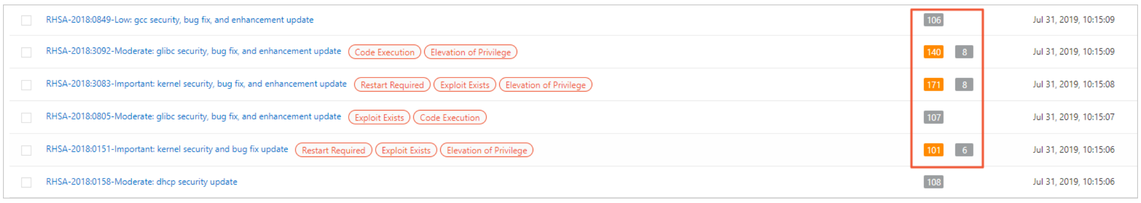
Vul Servers	Recommended Fix (CVE)	Fixing	Fixed Today	Total Fixed	Latest System Vul Time
263	167	5	32	4330	Aug 25, 2020, 14:22:56

□	Vulnerability	Affected Assets	Latest Scan Time	Actions
□	RHSA-2019:2136-Moderate: libssh2 security, bug fix, and enhancement update Remotely Exploitable 92,900	4	Aug 25, 2020, 08:47:19	Fix
□	RHEA-2018:0705 - Product Enhancement Advisory 36,900	4	Aug 25, 2020, 08:47:16	Fix
□	RHSA-2020:1000-Moderate: rsyslog security, bug fix, and enhancement update 119,800	4	Aug 25, 2020, 08:47:15	Fix
□	RHSA-2019:1884-Moderate: libssh2 security update Remotely Exploitable 565,900	4	Aug 25, 2020, 08:47:14	Fix

    - **View the priorities of vulnerabilities and the number of affected assets**

      The priorities of vulnerabilities are displayed in different colors in the Affected Assets column. The number in each row of the column indicates the total number of the assets affected by a vulnerability. The following list describes the relationship between colors and priorities:

        - Red: **High**
        - Orange: **Medium**
        - Gray: **Low**

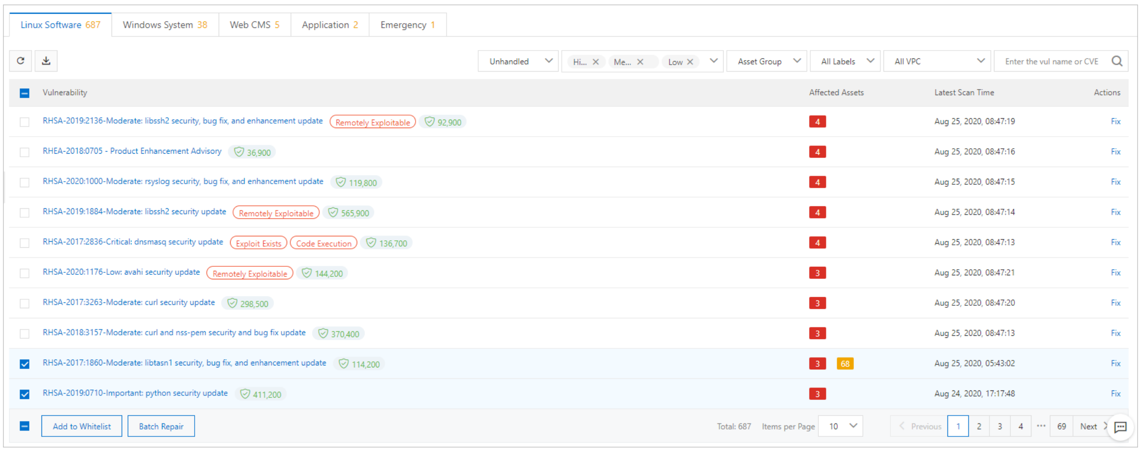


	Vulnerability		Affected Assets	Latest Scan Time
□	RHSA-2018:0849-Low: gcc security, bug fix, and enhancement update		106	Jul 31, 2019, 10:15:09
□	RHSA-2018:3092-Moderate: glibc security, bug fix, and enhancement update	Code Execution Elevation of Privilege	140 8	Jul 31, 2019, 10:15:09
□	RHSA-2018:3083-Important: kernel security, bug fix, and enhancement update	Restart Required Exploit Exists Elevation of Privilege	171 8	Jul 31, 2019, 10:15:08
□	RHSA-2018:0805-Moderate: glibc security, bug fix, and enhancement update	Exploit Exists Code Execution	107	Jul 31, 2019, 10:15:07
□	RHSA-2018:0151-Important: kernel security and bug fix update	Restart Required Exploit Exists Elevation of Privilege	101 6	Jul 31, 2019, 10:15:06
□	RHSA-2018:0158-Moderate: dhcp security update		108	Jul 31, 2019, 10:15:06

Note We recommend that you fix the vulnerabilities that have the **High** priority at the earliest opportunity.

- **Add vulnerabilities to the whitelist**

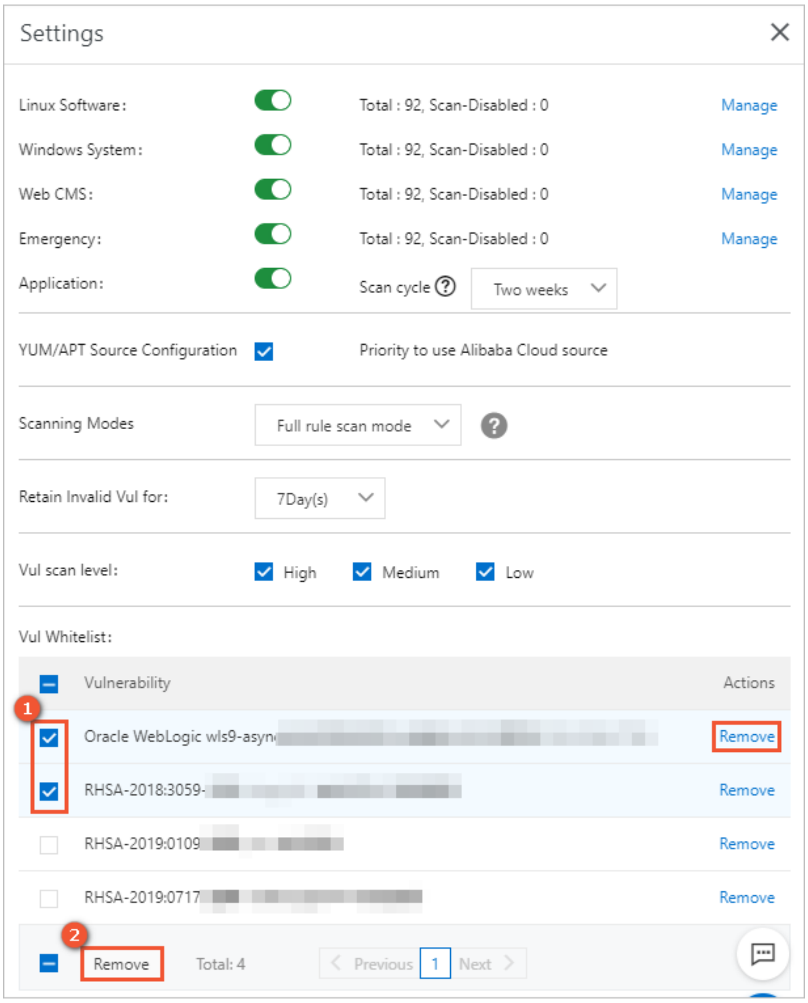
  On the **Linux Software** tab, select one or more vulnerabilities that you want to add to the whitelist and click **Add to Whitelist** below the vulnerability list. After you add the vulnerabilities to the whitelist, Security Center no longer generates alerts for the vulnerabilities.



☐	Vulnerability		Affected Assets	Latest Scan Time	Actions
□	RHSA-2019:2136-Moderate: libssh2 security, bug fix, and enhancement update	Remotely Exploitable 92,900	4	Aug 25, 2020, 08:47:19	Fix
□	RHEA-2018:0705 - Product Enhancement Advisory	36,900	4	Aug 25, 2020, 08:47:16	Fix
□	RHSA-2020:1000-Moderate: rsyslog security, bug fix, and enhancement update	119,800	4	Aug 25, 2020, 08:47:15	Fix
□	RHSA-2019:1884-Moderate: libssh2 security update	Remotely Exploitable 565,900	4	Aug 25, 2020, 08:47:14	Fix
□	RHSA-2017:2836-Critical: dnsmasq security update	Exploit Exists Code Execution 136,700	4	Aug 25, 2020, 08:47:13	Fix
□	RHSA-2020:1176-Low: avahi security update	Remotely Exploitable 144,200	3	Aug 25, 2020, 08:47:21	Fix
□	RHSA-2017:3263-Moderate: curl security update	298,500	3	Aug 25, 2020, 08:47:20	Fix
□	RHSA-2018:3157-Moderate: curl and nss-pem security and bug fix update	370,400	3	Aug 25, 2020, 08:47:13	Fix
☑	RHSA-2017:1860-Moderate: libtasn1 security, bug fix, and enhancement update	114,200	3 68	Aug 25, 2020, 05:43:02	Fix
☑	RHSA-2019:0710-Important: python security update	411,200	3	Aug 24, 2020, 17:17:48	Fix

  Vulnerabilities that are added to the whitelist are removed from the vulnerability list on the **Linux Software** tab. You can click **Settings** in the upper-right corner of the page to view the vulnerabilities in the **Vul Whitelist** section.

  If you want Security Center to detect and generate alerts for a vulnerability that is added to the whitelist, select the vulnerability in the Vul Whitelist section in the **Settings** panel and click **Remove**.



Settings

Linux Software:	●	Total : 92, Scan-Disabled : 0	Manage
Windows System:	●	Total : 92, Scan-Disabled : 0	Manage
Web CMS:	●	Total : 92, Scan-Disabled : 0	Manage
Emergency:	●	Total : 92, Scan-Disabled : 0	Manage
Application:	●	Scan cycle ? Two weeks	

YUM/APT Source Configuration ☑ Priority to use Alibaba Cloud source

Scanning Modes: Full rule scan mode

Retain Invalid Vul for: 7Day(s)

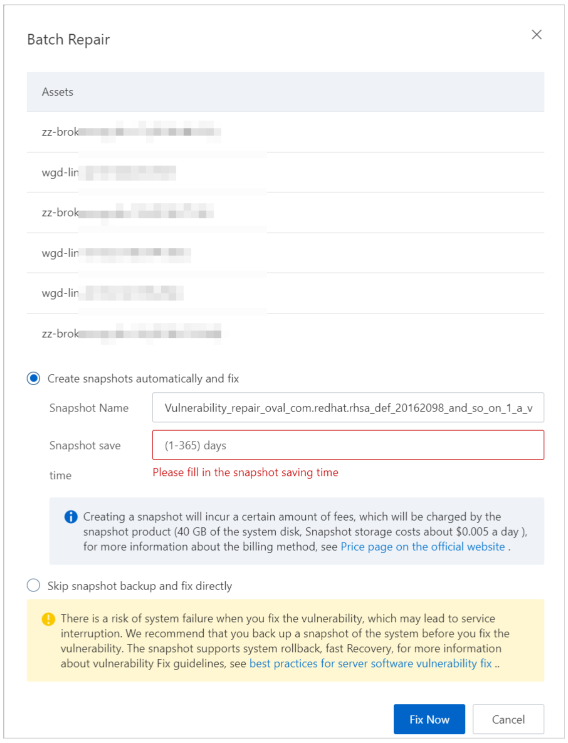
Vul scan level: ☑ High ☑ Medium ☑ Low

Vul Whitelist:

	Vulnerability	Actions
☑	Oracle WebLogic wls9-asyn[redacted]	Remove
☑	RHSA-2018:3059-[redacted]	Remove
□	RHSA-2019:0109[redacted]	Remove
□	RHSA-2019:0717[redacted]	Remove

- Fix multiple vulnerabilities at a time

If you fix multiple vulnerabilities at a time, Security Center automatically identifies affected assets and fixes the vulnerabilities on these assets. On the **Linux Software** tab, you can select the vulnerabilities that you want to fix at a time and click **Batch Repair**. In the **Batch Repair** dialog box, view the affected assets, select **Create snapshots automatically and fix** or **Skip snapshot backup and fix directly**, and then click **Fix Now**.



Batch Repair

Assets
zz-brok[redacted]
wgd-lin[redacted]
zz-brok[redacted]
wgd-lin[redacted]
wgd-lin[redacted]
zz-brok[redacted]

● Create snapshots automatically and fix

Snapshot Name: Vulnerability_repair_oval_com.redhat.rhsa_def_20162098_and_so_on_1_a_v

Snapshot save time: (1-365) days

Please fill in the snapshot saving time

Creating a snapshot will incur a certain amount of fees, which will be charged by the snapshot product (40 GB of the system disk, Snapshot storage costs about $0.005 a day), for more information about the billing method, see Price page on the official website .

○ Skip snapshot backup and fix directly

There is a risk of system failure when you fix the vulnerability, which may lead to service interruption. We recommend that you back up a snapshot of the system before you fix the vulnerability. The snapshot supports system rollback, fast Recovery, for more information about vulnerability Fix guidelines, see best practices for server software vulnerability fix ..

Notice

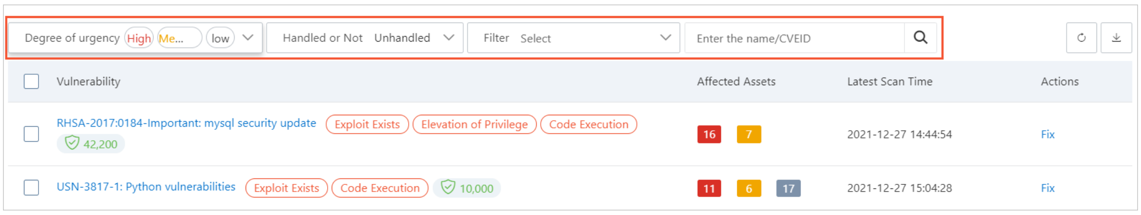
- You can select the vulnerabilities only on the current page. A total of 10, 20, or 50 vulnerabilities can be displayed on each page. Therefore, you can fix up to 50 vulnerabilities at a time.
- For outdated or commercial operating systems, you must manually upgrade the operating systems to fix vulnerabilities. Security Center cannot fix multiple vulnerabilities that are detected on the operating systems at a time. After you use the Batch Repair feature to fix the vulnerabilities, Security Center ignores the vulnerabilities. If you use one of the following operating systems, you must upgrade your operating system to fix multiple vulnerabilities at a time:
  - Red Hat 5, Red Hat 6, Red Hat 7, and Red Hat 8
  - CentOS 5
  - Ubuntu 12
- The system may fail to fix a vulnerability. Before you click Fix Now, we recommend that you select **Create snapshots automatically and fix** to create a snapshot of the system. For more information about Elastic Compute Service (ECS) snapshots, see Snapshot overview.
- You are charged based on the billing methods of the snapshot service.For example, if the size of the system disk is 40 GB, the fees for snapshot storage are USD 0.005 per day. For more information, see Snapshots.

- **Search for vulnerabilities**

  On the **Linux Software** tab, you can search for vulnerabilities by using or combining the following methods:

  - Search for vulnerabilities by priority. The priority can be **High**, **Medium**, or **low**.
  - Search for vulnerabilities by status. The status can be **Handled** or **Unhandled**.
  - Search for vulnerabilities by **Asset group**, **VPC**, or **Tags**.
  - Enter the name or Common Vulnerabilities and Exposures (CVE) ID of a vulnerability in the search box.

    > **Note** If you search for vulnerabilities by name, fuzzy match is supported.



Degree of urgency High Me... low | Handled or Not Unhandled | Filter Select | Enter the name/CVEID

□	Vulnerability	Affected Assets	Latest Scan Time	Actions
□	RHSA-2017:0184-Important: mysql security update Exploit Exists Elevation of Privilege Code Execution 42,200	16 7	2021-12-27 14:44:54	Fix
□	USN-3817-1: Python vulnerabilities Exploit Exists Code Execution 10,000	11 6 17	2021-12-27 15:04:28	Fix

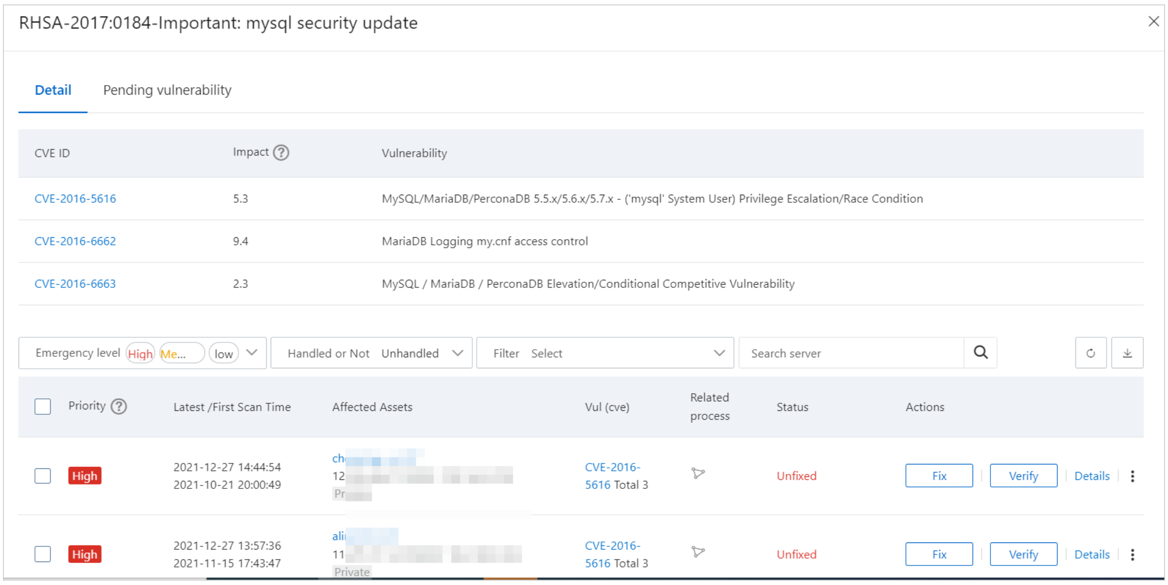
- **Export vulnerabilities**

  In the upper-right corner of the **Linux Software** tab, you can click the ⤓ icon to export and save all detected vulnerabilities to your computer. The exported file is in the Excel format.

  > **Note** The time that is required to export the vulnerabilities varies based on the size of vulnerability data.

View and handle vulnerabilities

1.
2.
3. On the **Vulnerabilities** page, click the **Linux Software** tab.
4. On the Linux Software tab, find the vulnerability that you want to view. Click the vulnerability name in the **Vulnerability** column or **Fix** in the **Actions** column. The panel that shows the vulnerability details appears.
5. In the panel, view and handle the vulnerability.



RHSA-2017:0184-Important: mysql security update

CVE ID	Impact	Vulnerability
CVE-2016-5616	5.3	MySQL/MariaDB/PerconaDB 5.5.x/5.6.x/5.7.x - ('mysql' System User) Privilege Escalation/Race Condition
CVE-2016-6662	9.4	MariaDB Logging my.cnf access control
CVE-2016-6663	2.3	MySQL / MariaDB / PerconaDB Elevation/Conditional Competitive Vulnerability

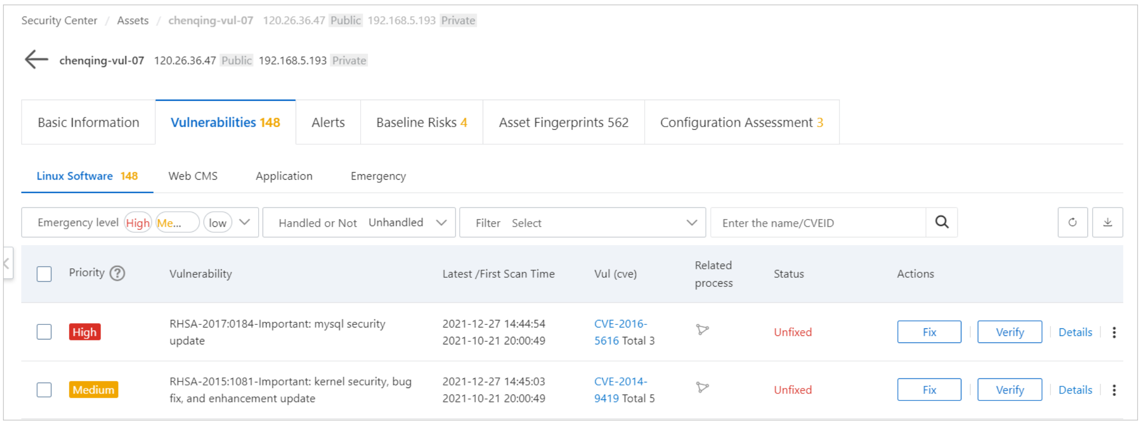
Emergency level High Me... low · Handled or Not Unhandled · Filter Select · Search server

□ Priority	Latest /First Scan Time	Affected Assets	Vul (cve)	Related process	Status	Actions
□ High	2021-12-27 14:44:54 2021-10-21 20:00:49	[redacted]	CVE-2016-5616 Total 3		Unfixed	Fix Verify Details
□ High	2021-12-27 13:57:36 2021-11-15 17:43:47	[redacted]	CVE-2016-5616 Total 3		Unfixed	Fix Verify Details

You can perform the following operations:

- **View vulnerability details**
  - On the **Detail** tab, view all vulnerabilities that are associated with the vulnerability and all assets that are affected by the vulnerability. You can also analyze all vulnerabilities and handle multiple vulnerabilities at a time.
  - On the **Pending vulnerability** tab, view the assets that are affected by the vulnerability. You can view all assets that are affected by the vulnerability and the status of the vulnerability that affects specific assets. You can fix a vulnerability, ignore a vulnerability, or add a vulnerability to a whitelist. You can also verify or undo a vulnerability fix.

  On the Detail tab, click an asset in the **Affected Assets** column to go to the **Vulnerabilities** tab of the **Assets** page. On this tab, you can view the information about all Linux software vulnerabilities that are associated with this asset.



Security Center / Assets / chenqing-vul-07 120.26.36.47 Public 192.168.5.193 Private

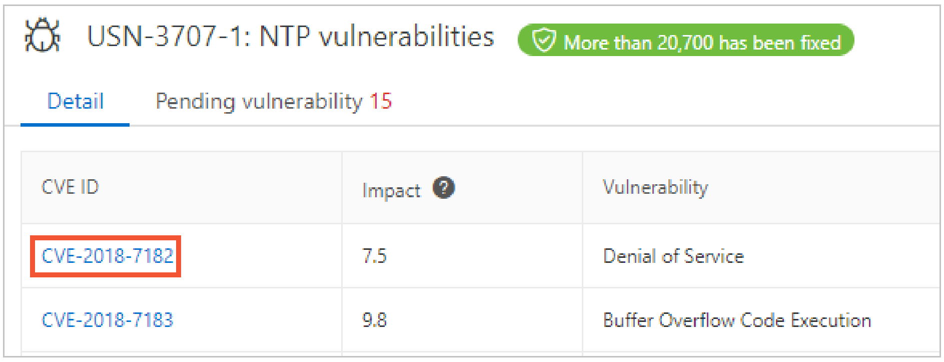
chenqing-vul-07 120.26.36.47 Public 192.168.5.193 Private

Emergency level High Me... low · Handled or Not Unhandled · Filter Select · Enter the name/CVEID

□ Priority	Vulnerability	Latest /First Scan Time	Vul (cve)	Related process	Status	Actions
□ High	RHSA-2017:0184-Important: mysql security update	2021-12-27 14:44:54 2021-10-21 20:00:49	CVE-2016-5616 Total 3		Unfixed	Fix Verify Details
□ Medium	RHSA-2015:1081-Important: kernel security, bug fix, and enhancement update	2021-12-27 14:45:03 2021-10-21 20:00:49	CVE-2014-9419 Total 5		Unfixed	Fix Verify Details

- **View the details about the Alibaba Cloud vulnerability library**

On the **Detail** tab, click the ID of a vulnerability that you want to fix in the **CVE ID** column to go to the Alibaba Cloud vulnerability library.



USN-3707-1: NTP vulnerabilities

CVE ID	Impact	Vulnerability
CVE-2018-7182	7.5	Denial of Service
CVE-2018-7183	9.8	Buffer Overflow Code Execution

This library displays detailed information about the vulnerability, including the vulnerability description, basic information, and solution.

- **View vulnerability priorities**
  Vulnerability priorities are marked in different colors:
  - Red: **High**
  - Orange: **Medium**
  - Gray: **Low**

  Note We recommend that you fix the vulnerabilities that have the **High** priority at the earliest opportunity.

- **View the processes related to vulnerability fixes**
  On the Pending vulnerability tab, click the icon in the **Related process** column to view the processes that are related to the vulnerability. In the panel that appears, you can view the processes or business systems that may be affected by the vulnerability fix.

- **View the vulnerability status**
  The status of a vulnerability can be Handled or Unhandled.
  - **Handled**
    - **Handled**: The vulnerability is fixed.
    - **Ignored**: The vulnerability is ignored. Security Center no longer generates alerts on this vulnerability.

    Note You can use snapshots to undo a vulnerability fix for a **Handled** vulnerability. After you undo a vulnerability fix, the status of the vulnerability changes to **Unhandled**.

- **Unhandled**
  - **Unfixed**: The vulnerability is to be fixed.
  - **Fixing**: The vulnerability is being fixed.
  - **Fix Failed**: Security Center failed to fix the vulnerability. The file that contains the vulnerability data may have been modified or does not exist.
  - **Handled (To Be Restarted)**: The vulnerability is fixed. You must restart the system for the fix to take effect.
  - **Verifying**: The vulnerability has been fixed. If a system restart is required, you can verify the fix after you restart the system.

- **Handle the vulnerabilities of the affected assets**

  On the Pending vulnerability tab, you can fix or ignore a vulnerability. You can also verify or undo a vulnerability fix.

  > ? **Note** If you want to handle the vulnerability on all affected assets, select all affected assets and perform the required operations. To select all affected assets with a few clicks, you can select the check box next to **Vulnerability**.

  You can perform the following operations based on your business requirements:

  - **Fix vulnerabilities**

    Fix vulnerabilities based on the following scenarios:

    - The **Fix** button is available

      Select one or more associated vulnerabilities and click **Fix**. Security Center can automatically create snapshots and fix vulnerabilities. You can select **Create snapshots automatically and fix** or **Skip snapshot backup and fix directly** based on your business requirements.

      > ? **Note**
      >
      > - The system may fail to fix a vulnerability. Before you click Fix Now, we recommend that you select **Create snapshots automatically and fix** to create a snapshot of the system. For more information about Elastic Compute Service (ECS) snapshots, see Snapshot overview.
      > - You are charged based on the billing methods of the snapshot service.For example, if the size of the system disk is 40 GB, the fees for snapshot storage are USD 0.005 per day. For more information, see Snapshots.

- The **Fix** button is dimmed
  The button is dimmed in the following scenarios:
  - For outdated or commercial operating systems, you must manually upgrade the operating systems to fix vulnerabilities.

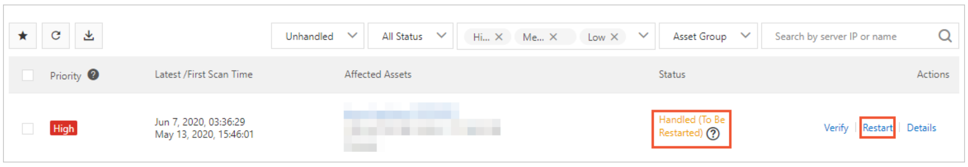
    > Note If you use one of the following operating systems, you must upgrade your operating system to fix vulnerabilities:
    > - Red Hat 5, Red Hat 6, Red Hat 7, and Red Hat 8
    > - CentOS 5
    > - Ubuntu 12

  - Linux software vulnerabilities may fail to be fixed due to issues, such as insufficient disk space on your server or unauthorized access to files. Before you fix Linux software vulnerabilities in the Security Center console, you must manually handle the issues on the server. The following list describes these issues and solutions:
    - The disk space is smaller than 3 GB.
    - The apt-get or APT/YUM process is running.
      Solution: Wait until the process is complete, or manually stop the process. Then, fix the vulnerability again in the Security Center console.
    - Insufficient permissions to run the APT, YUM, or RPM command.
      Solution: Check and manage access permissions on the files. We recommend that you set file permissions to 755, and make sure that the file owner is the root user. Then, fix the vulnerability again in the Security Center console.

      > Note After you set file permissions to 755, the file owner has the read, write, and execute permissions on the file. Other users and the user group to which the file owner belongs have read and execute permissions on the file.

  To view server issues, move the pointer over the **Fix** button. The suggestions are provided by Security Center.

- **Restart the system**
  After you fix Linux kernel vulnerabilities, you must restart the system. You can use one of the following methods to restart the system:
  - (Recommended) Click **Restart** on the Detail tab.



□	Priority ?	Latest /First Scan Time	Affected Assets	Status	Actions
□	High	Jun 7, 2020, 03:36:29 May 13, 2020, 15:46:01	[redacted]	Handled (To Be Restarted) ?	Verify | Restart | Details

  > Note If the system has vulnerabilities that are in the fixing or verifying state, you cannot restart the system. In this case, if you click **Restart**, an error message appears. The error message indicates that the system restart fails. Before you restart a system, make sure that no vulnerabilities are in the fixing or verifying state.

  - Run the required command in the Linux system.

  - **Verify a vulnerability fix**

    Select a vulnerability or multiple associated vulnerabilities and click **Verify** to check whether the vulnerabilities are fixed.

    After you click **Verify**, the **Status** of the vulnerability changes to **Verifying**. The fix can be verified after several seconds.

  - **Ignore a vulnerability**

    Find the vulnerability that you want to ignore, click the ⋮ icon in the **Actions** column, and then select **Ignore**. In the dialog box that appears, enter the description for the ignore operation and click **OK**. After a vulnerability is ignored, Security Center no longer generates alerts for the vulnerability.

    Search for **Handled** vulnerabilities, find the vulnerability that is ignored, and then click the vulnerability to go to the panel that shows the vulnerability details. In the panel, move the pointer over the ? icon in the Status column to view the description of the ignore operation.

    > **Note** The state of this vulnerability changes to **Ignored**. If you want Security Center to generate alerts on an ignored vulnerability, find the vulnerability in the **Handled** vulnerability list and click **Unignore** in the panel.

  - **Undo a vulnerability fix**

    Find the vulnerability for which you want to undo the fix, click **Rollback** in the **Actions** column. In the **Rollback** dialog box, select the snapshot that you want to use to undo the fix and click **OK**.

- **Search for affected assets**

  On the Pending vulnerability tab, you can search for affected assets by vulnerability priority, VPC name, asset group, vulnerability status, server IP address, or server name. The vulnerability priority can be high, medium, or low. The vulnerability status can be handled or unhandled.

  > **Note** If you search for affected assets by server IP address or name, fuzzy match is supported.

- **Export affected assets**

  In the upper-left corner of the Pending vulnerability tab, click the ⤓ icon to export and save all affected assets to your computer. The exported file is in the Excel format.

  > **Note** The time that is required to export the vulnerabilities varies based on the size of asset data.

Description of the panel that shows the vulnerability details

Parameter	Description
CVE ID	The CVE ID of the vulnerability. The CVE system provides a reference method for publicly known information-security vulnerabilities and exposures. You can use CVE IDs, such as *CVE-2018-1123*, to query relevant information about vulnerability fixes in databases that are compatible with CVE. This way, security issues can be resolved.

Parameter	Description
Impact	The value of the Impact parameter is a Common Vulnerability Scoring System (CVSS) score. The CVSS score follows the widely accepted industry standard and is calculated by using the formula that depends on several attributes of the vulnerability. This score is used to determine the severity of the vulnerability. The following list describes the severity rating scale in CVSS v3.0: ● 0: none ● 0.1 to 3.9: low ○ Vulnerabilities that cause local DDoS attacks ○ Vulnerabilities that have minor impacts ● 4.0 to 6.9: medium ○ Vulnerabilities that affect users only when the system and user interacts ○ Vulnerabilities that attackers can exploit to perform unauthorized operations ○ Vulnerabilities that can be exploited after attackers change local configurations or obtain the required information ● 7.0 to 8.9: high ○ Vulnerabilities that attackers can exploit to indirectly obtain permissions on your server and application systems ○ Vulnerabilities that attackers can exploit to read, write, download, or delete files ○ Vulnerabilities that cause sensitive data leaks ○ Vulnerabilities that cause service interruptions or remote DDoS attacks ● 9.0 to 10.0: critical ○ Vulnerabilities that attackers can exploit to directly obtain permissions on your server ○ Vulnerabilities that attackers can exploit to directly obtain sensitive data and cause data leaks ○ Vulnerabilities that cause unauthorized access to sensitive data ○ Vulnerabilities that cause large-scale impacts
Affected Assets	The details about assets that are affected by the vulnerability, including the public and private IP addresses of the assets.
Priority	The vulnerability priority. The following items describe the priorities: ● **High** We recommend that you fix high-priority vulnerabilities at the earliest opportunity. ● **Medium** You can fix medium-priority vulnerabilities based on your business requirements. ● **Low** You can fix or ignore low-priority vulnerabilities based on your business requirements.

Parameter	Description
Details	In the panel, find a vulnerability and click **Details** in the **Actions** column to view the details about the vulnerability. ● **Fix Command**: the command that you can run to fix the vulnerability. ● **Impact description**: ○ **Software**: the version of the software on the current server. ○ **Cause**: the reason why the software has the vulnerability. In most cases, the vulnerability is detected due to the outdated version of the software. ○ **Path**: the path of the software on the server. ● **Caution**: important notes, prevention tips, and references for the vulnerability.

1.4. View and handle Windows system vulnerabilities

Security Center can detect and fix Windows system vulnerabilities. This topic describes how to view and handle Windows system vulnerabilities.

Context

Security Center synchronizes security updates from the Microsoft official website in real time. This allows Security Center to effectively detect high-risk vulnerabilities and generate alerts. This also prevents attackers from exploiting Windows system vulnerabilities that compromise the security of your servers.

> **Note** The and editions of Security Center detect but do not fix vulnerabilities. To use Security Center to fix vulnerabilities with a few clicks, you must purchase the , , or edition. For more information about the features supported by different Security Center editions, see Features.

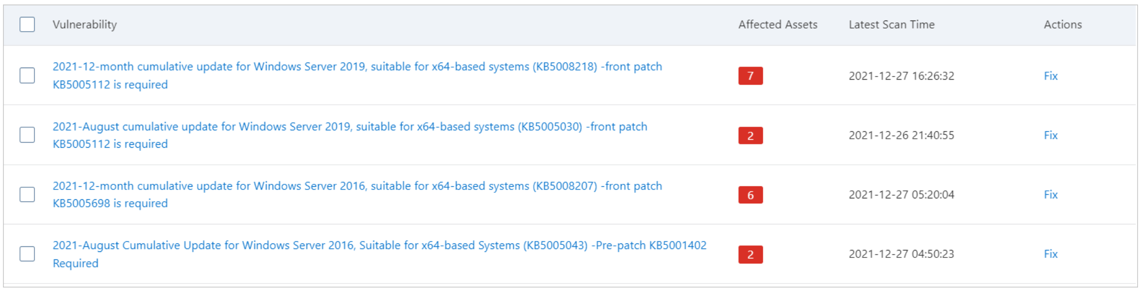
View the basic information about a vulnerability

1.
2.
3.
4. On the **Windows System** tab, view and handle all Windows system vulnerabilities that are detected by Security Center.

   You can perform the following operations on the tab:

   - **View vulnerability details**

In the vulnerability list of the **Windows System** tab, you can view vulnerability details.



☐ Vulnerability	Affected Assets	Latest Scan Time	Actions
☐ 2021-12-month cumulative update for Windows Server 2019, suitable for x64-based systems (KB5008218) -front patch KB5005112 is required	7	2021-12-27 16:26:32	Fix
☐ 2021-August cumulative update for Windows Server 2019, suitable for x64-based systems (KB5005030) -front patch KB5005112 is required	2	2021-12-26 21:40:55	Fix
☐ 2021-12-month cumulative update for Windows Server 2016, suitable for x64-based systems (KB5008207) -front patch KB5005698 is required	6	2021-12-27 05:20:04	Fix
☐ 2021-August Cumulative Update for Windows Server 2016, Suitable for x64-based Systems (KB5005043) -Pre-patch KB5001402 Required	2	2021-12-27 04:50:23	Fix

- **View vulnerability priorities**

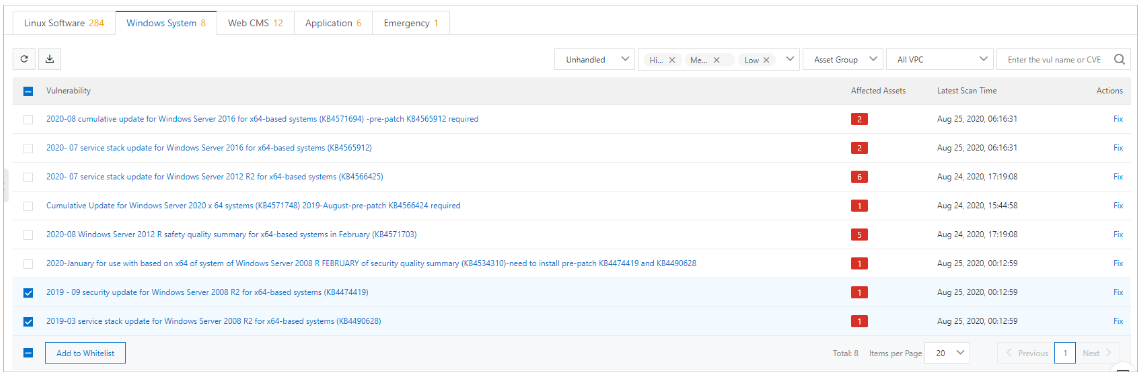
  The priorities of vulnerabilities are displayed in different colors in the Affected Assets column. The number in each row of the column indicates the total number of the assets affected by a vulnerability. The following list describes the relationship between colors and priorities:

  - Red: **High**
  - Orange: **Medium**
  - Gray: **Low**

  > **Note** We recommend that you fix vulnerabilities that have the **High** priority at the earliest opportunity.

- **Add vulnerabilities to the whitelist**

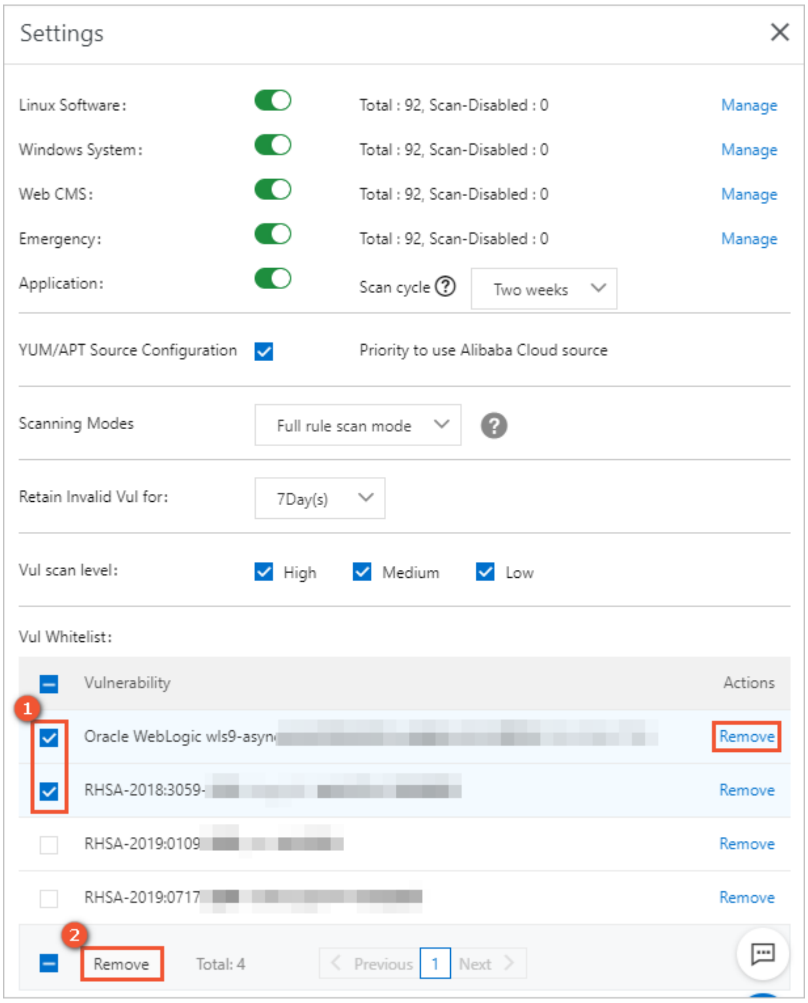
  On the **Windows System** tab, you can select vulnerabilities and click **Add to Whitelist** to add them to the whitelist. After you add the vulnerabilities to the whitelist, Security Center no longer generates alerts for the vulnerabilities.



▬ Vulnerability	Affected Assets	Latest Scan Time	Actions
☐ 2020-08 cumulative update for Windows Server 2016 for x64-based systems (KB4571694) -pre-patch KB4565912 required	2	Aug 25, 2020, 06:16:31	Fix
☐ 2020- 07 service stack update for Windows Server 2016 for x64-based systems (KB4565912)	2	Aug 25, 2020, 06:16:31	Fix
☐ 2020- 07 service stack update for Windows Server 2012 R2 for x64-based systems (KB4566425)	6	Aug 24, 2020, 17:19:08	Fix
☐ Cumulative Update for Windows Server 2020 x 64 systems (KB4571748) 2019-August-pre-patch KB4566424 required	1	Aug 24, 2020, 15:44:58	Fix
☐ 2020-08 Windows Server 2012 R safety quality summary for x64-based systems in February (KB4571703)	5	Aug 24, 2020, 17:19:08	Fix
☐ 2020-January for use with based on x64 of system of Windows Server 2008 R FEBRUARY of security quality summary (KB4534310)-need to install pre-patch KB4474419 and KB4490628	1	Aug 25, 2020, 00:12:59	Fix
☑ 2019 - 09 security update for Windows Server 2008 R2 for x64-based systems (KB4474419)	1	Aug 25, 2020, 00:12:59	Fix
☑ 2019-03 service stack update for Windows Server 2008 R2 for x64-based systems (KB4490628)	1	Aug 25, 2020, 00:12:59	Fix

After you add vulnerabilities to the whitelist, these vulnerabilities are removed from the vulnerability list on the **Windows System** tab. You can click **Settings** in the upper-right corner of the page to view these vulnerabilities in the **Vul Whitelist** section.

If you want Security Center to detect and generate alerts for a vulnerability that is added to the whitelist, select the vulnerability in the Vul Whitelist section in the **Settings** panel and click **Remove**.



Settings

Linux Software:	On	Total : 92, Scan-Disabled : 0	Manage
Windows System:	On	Total : 92, Scan-Disabled : 0	Manage
Web CMS:	On	Total : 92, Scan-Disabled : 0	Manage
Emergency:	On	Total : 92, Scan-Disabled : 0	Manage
Application:	On	Scan cycle: Two weeks	

YUM/APT Source Configuration ☑ Priority to use Alibaba Cloud source

Scanning Modes: Full rule scan mode

Retain Invalid Vul for: 7Day(s)

Vul scan level: ☑ High ☑ Medium ☑ Low

Vul Whitelist:

	Vulnerability	Actions
☑	Oracle WebLogic wls9-asyn[redacted]	Remove
☑	RHSA-2018:3059-[redacted]	Remove
□	RHSA-2019:0109[redacted]	Remove
□	RHSA-2019:0717[redacted]	Remove

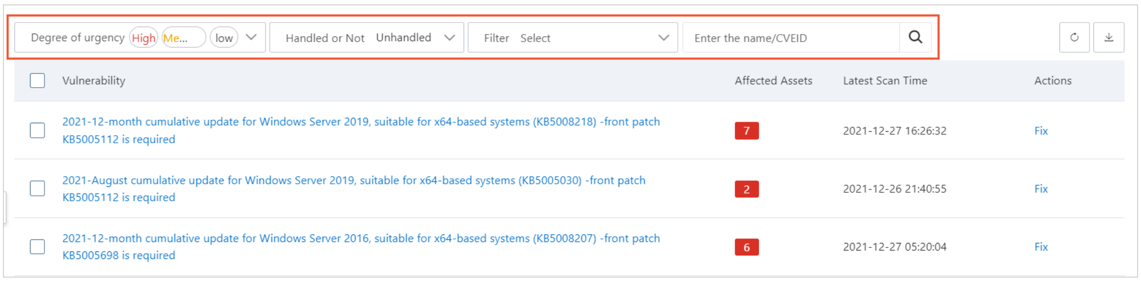
Remove Total: 4 Previous 1 Next

- **Search for vulnerabilities**

  On the **Windows System** tab, you can search for vulnerabilities by using or combining the following methods:

  - Search for vulnerabilities by priority. The priority can be **High**, **Medium**, or **low**.
  - Search for vulnerabilities by status. The status can be **Handled** or **Unhandled**.
  - Search for vulnerabilities by **Asset group**, **VPC**, or **Tags**.
  - Enter the name or Common Vulnerabilities and Exposures (CVE) ID of a vulnerability in the search box.

  > **Note** If you search for vulnerabilities by name, fuzzy match is supported.



Degree of urgency High Me... low | Handled or Not Unhandled | Filter Select | Enter the name/CVEID

	Vulnerability	Affected Assets	Latest Scan Time	Actions
□	2021-12-month cumulative update for Windows Server 2019, suitable for x64-based systems (KB5008218) -front patch KB5005112 is required	7	2021-12-27 16:26:32	Fix
□	2021-August cumulative update for Windows Server 2019, suitable for x64-based systems (KB5005030) -front patch KB5005112 is required	2	2021-12-26 21:40:55	Fix
□	2021-12-month cumulative update for Windows Server 2016, suitable for x64-based systems (KB5008207) -front patch KB5005698 is required	6	2021-12-27 05:20:04	Fix

- **Export vulnerabilities**

On the **Windows System** tab, you can click the ⤓ icon to export and save all detected Windows system vulnerabilities to your computer. The exported file is in the Excel format.

> **Note** The time that is required to export the vulnerabilities varies based on the size of vulnerability data.

View vulnerability details and handle vulnerabilities

1.
2.
3.
4. In the **Vulnerability** column, click the name of the vulnerability that you want to handle, or click **Fix** in the **Actions** column of the vulnerability that you want to handle to go to the panel that shows the vulnerability details.

   In the panel, you can view the details about vulnerabilities on the **Detail** tab. You can also view the number of unhandled vulnerabilities and affected assets on the **Pending vulnerability** tab.

5. In the panel, view and handle vulnerabilities.

   You can perform the following operations:

   - **View vulnerability details**
     - On the **Detail** tab, you can view all the affected assets and vulnerabilities related to the vulnerability. You can also analyze and handle multiple related vulnerabilities at a time.
     - On the **Pending vulnerability** tab, you can view the assets that are affected by the vulnerability.
       You can view the assets affected by the vulnerability and the status of the vulnerability. You can fix or ignore a vulnerability. You can also verify a vulnerability fix or add a vulnerability to the whitelist.
   - **View vulnerability priorities**
     For more information about the priorities of Windows system vulnerabilities, visit the Microsoft official website. Vulnerability priorities are marked in different colors:
     - Red: **High**. The equivalent severity at the Microsoft official website is **Critical** or **Important**.
     - Orange: **Medium**. The equivalent severity at the Microsoft official website is **Moderate**.
     - Gray: **Low**. The equivalent severity at the Microsoft official website is **Low**.

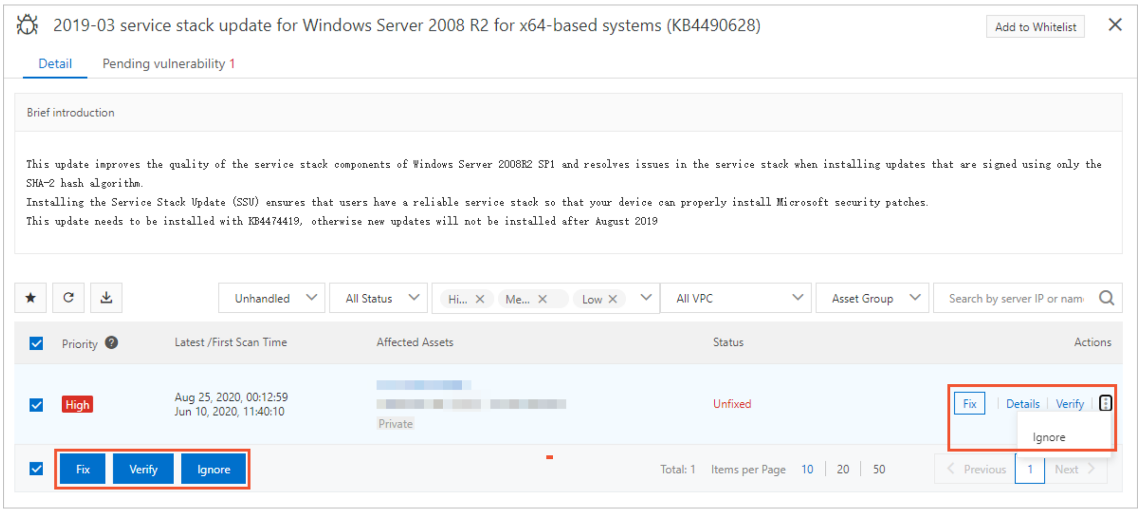
     > **Note** We recommend that you fix the vulnerabilities that have the **High** priority at the earliest opportunity.

   - **View vulnerability status**
     - **Handled**
       - **Handled**: The vulnerability is fixed.
       - **Ignored**: The vulnerability is ignored. Security Center no longer generates alerts on this vulnerability.

- **Unhandled**
  - **Unfixed**: The vulnerability is to be fixed.
  - **Fixing**: The vulnerability is being fixed.
  - **Fix Failed**: Security Center failed to fix the vulnerability. The file that contains the vulnerability data may have been modified or does not exist.
  - Verifying: After you start the verification, the state of the vulnerability changes to Verifying.

- **Handle the vulnerabilities of the affected assets**

  You can fix or ignore a vulnerability. You can also verify a vulnerability fix or add a vulnerability to the whitelist.



2019-03 service stack update for Windows Server 2008 R2 for x64-based systems (KB4490628)

Brief introduction

This update improves the quality of the service stack components of Windows Server 2008R2 SP1 and resolves issues in the service stack when installing updates that are signed using only the SHA-2 hash algorithm.
Installing the Service Stack Update (SSU) ensures that users have a reliable service stack so that your device can properly install Microsoft security patches.
This update needs to be installed with KB4474419, otherwise new updates will not be installed after August 2019

Priority	Latest /First Scan Time	Affected Assets	Status	Actions
High	Aug 25, 2020, 00:12:59 Jun 10, 2020, 11:40:10	[redacted] Private	Unfixed	Fix | Details | Verify | Ignore

Total: 1 Items per Page 10 | 20 | 50

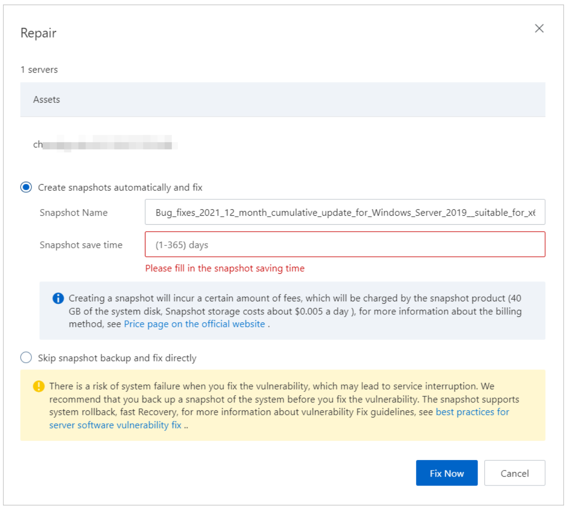
You can perform the following operations:

- **Fix vulnerabilities**

  Fix vulnerabilities based on the following scenarios:

- The **Fix** button is available
  Select one or more associated vulnerabilities and click **Fix**. Security Center can automatically create snapshots and fix vulnerabilities. You can select **Create snapshots automatically and fix** or **Skip snapshot backup and fix directly** based on your business requirements.

  > **Note**
  >
  > - The system may fail to fix a vulnerability. Before you click Fix Now, we recommend that you select **Create snapshots automatically and fix** to create a snapshot of the system. For more information about Elastic Compute Service (ECS) snapshots, see Snapshot overview.
  > - You are charged based on the billing methods of the snapshot service.For example, if the size of the system disk is 40 GB, the fees for snapshot storage are USD 0.005 per day. For more information, see Snapshots.

  Repair

  1 servers

  Assets

  ch[redacted]

  ● Create snapshots automatically and fix

  Snapshot Name: Bug_fixes_2021_12_month_cumulative_update_for_Windows_Server_2019__suitable_for_x6

  Snapshot save time: (1-365) days

  Please fill in the snapshot saving time

  Creating a snapshot will incur a certain amount of fees, which will be charged by the snapshot product (40 GB of the system disk, Snapshot storage costs about $0.005 a day), for more information about the billing method, see Price page on the official website .

  ○ Skip snapshot backup and fix directly

  There is a risk of system failure when you fix the vulnerability, which may lead to service interruption. We recommend that you back up a snapshot of the system before you fix the vulnerability. The snapshot supports system rollback, fast Recovery, for more information about vulnerability Fix guidelines, see best practices for server software vulnerability fix ..

- The **Fix** button is dimmed
  If the disk space of a server is insufficient or the Windows Update service is running, the vulnerabilities fail to be fixed and the Fix button is dimmed. To fix the vulnerabilities, you must handle the issues on the server. To view the server issues and solutions provided by Security Center, move the pointer over the **Fix** button. You must manually handle the following issues:
  - The Windows Update service is running.
    Solution: Wait for a few minutes and try to fix the vulnerabilities again. Alternatively, terminate the Wusa process on the server and try to fix the vulnerabilities again in the Security Center console.
  - The Windows Update service is disabled.
    Solution: Start Task Manager of the server and enable the Windows Update service. Then, try to fix the vulnerabilities again in the Security Center console.
  - The server disk space is less than 500 MB.
    Solution: Resize or clear the disk. Then, try to fix the vulnerabilities again in the Security Center console.

- - **Verify a vulnerability fix**

    Select a vulnerability or multiple associated vulnerabilities and click **Verify** to check whether the vulnerabilities are fixed.

    After you click **Verify**, the **Status** of the vulnerability changes to **Verifying**. The fix can be verified after several seconds.

  - **Add vulnerabilities to the whitelist**

    On the **Windows System** tab, you can select vulnerabilities and click **Add to Whitelist** to add them to the whitelist. After you add the vulnerabilities to the whitelist, Security Center no longer generates alerts for the vulnerabilities.

    After you add vulnerabilities to the whitelist, these vulnerabilities are removed from the vulnerability list on the **Windows System** tab. You can click **Settings** in the upper-right corner of the page to view these vulnerabilities in the **Vul Whitelist** section.

    If you want Security Center to detect and generate alerts for a vulnerability that is added to the whitelist, select the vulnerability in the Vul Whitelist section in the **Settings** panel and click **Remove**.

  - **Ignore a vulnerability**

    Find the vulnerability that you want to ignore, click the ⋮ icon in the **Actions** column, and then select **Ignore**. In the dialog box that appears, enter the description for the ignore operation and click **OK**. After a vulnerability is ignored, Security Center no longer generates alerts for the vulnerability.

    Search for **Handled** vulnerabilities, find the vulnerability that is ignored, and then click the vulnerability to go to the panel that shows the vulnerability details. In the panel, move the pointer over the ? icon in the Status column to view the description of the ignore operation.

    > **Note** The state of this vulnerability changes to **Ignored**. If you want Security Center to generate alerts on an ignored vulnerability, find the vulnerability in the **Handled** vulnerability list and click **Unignore** in the panel.

- **Search for affected assets**

  On the Pending vulnerability tab, you can search for affected assets by vulnerability priority, VPC name, asset group, vulnerability status, server IP address, or server name. The vulnerability priority can be high, medium, or low. The vulnerability status can be handled or unhandled.

  > **Note** If you search for affected assets by server IP address or name, fuzzy match is supported.

- **Export affected assets**

  In the upper-left corner of the Pending vulnerability tab, click the ⤓ icon to export and save all affected assets to your computer. The exported file is in the Excel format.

  > **Note** The time that is required to export the vulnerabilities varies based on the size of asset data.

References

The "0x80240017 104 (Patch Not Applicable)" error is returned when you fix Windows system vulnerabilities. How do I handle the issue?

1.5. View and handle Web-CMS vulnerabilities

Security Center can detect and fix Web-CMS vulnerabilities. The feature of Web-CMS vulnerability detection monitors website directories and identifies common website builders. This feature compares vulnerability files with the vulnerability library to detect the vulnerabilities in website builders. This topic describes how to view and handle Web-CMS vulnerabilities.

Context

The feature of Web-CMS vulnerability detection obtains information about the latest Web-CMS vulnerabilities and patches, and delivers the patches. This allows you to detect and fix Web-CMS vulnerabilities at the earliest opportunity. This feature detects vulnerabilities in a timely manner, fixes vulnerabilities, and applies patches to fix multiple vulnerabilities at a time.

> **Note**
>
> - The and editions of Security Center detect but do not fix vulnerabilities. To use Security Center to fix vulnerabilities with a few clicks, you must purchase the , , or edition. For more information about the features supported by different Security Center editions, see Features.
> - After you fix Web-CMS vulnerabilities in the Security Center console, the fixes immediately take effect. You do not need to verify the fixes.

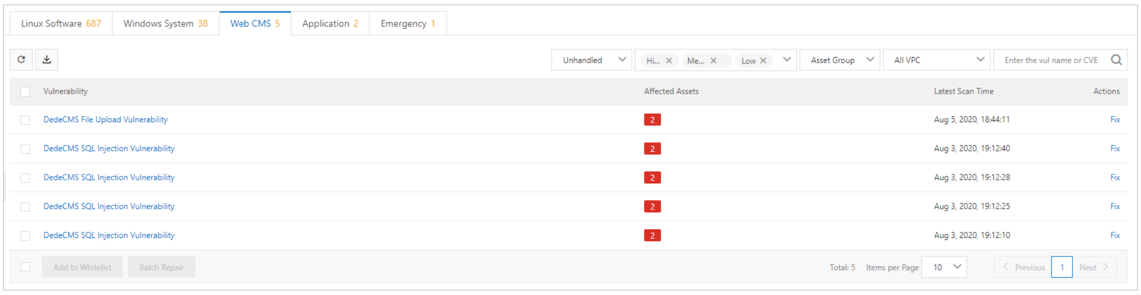
For more information about the Web-CMS vulnerabilities that can be detected by Security Center, see Web-CMS vulnerabilities that can be detected.

View the basic information about a vulnerability

1.
2.
3.
4. On the **Web CMS** tab, view the information about all Web-CMS vulnerabilities detected by Security Center.

   You can perform the following operations on the tab:

   - **View vulnerability information**

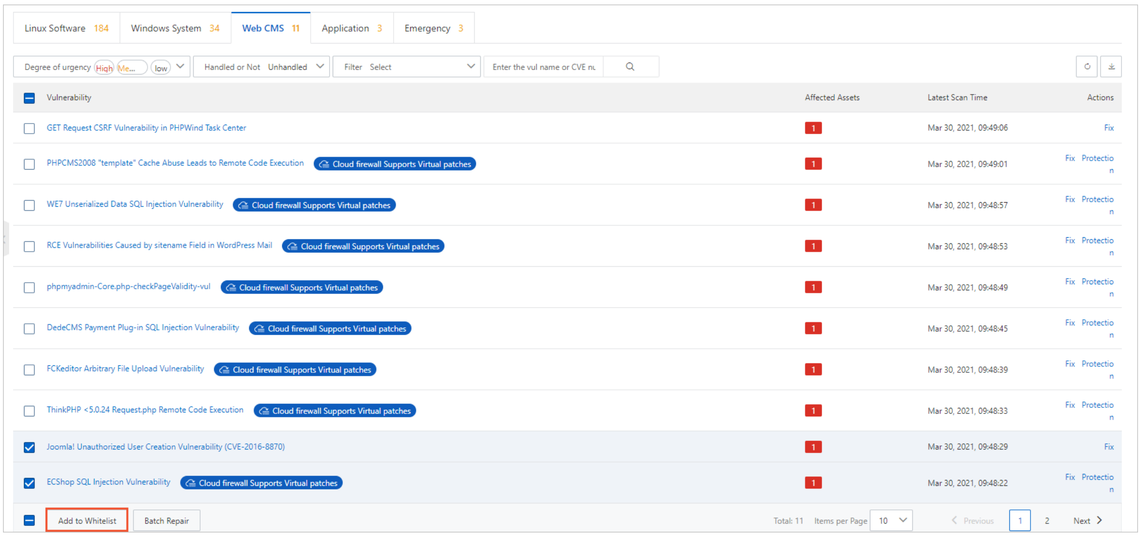
     

Vulnerability	Affected Assets	Latest Scan Time	Actions
DedeCMS File Upload Vulnerability	2	Aug 5, 2020, 18:44:11	Fix
DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:40	Fix
DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:28	Fix
DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:25	Fix
DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:10	Fix

   - **View vulnerability priorities**
     All Web-CMS vulnerabilities can cause serious damage. This is confirmed by Alibaba Cloud security engineers. Therefore, the priorities of detected Web-CMS vulnerabilities are **High** and marked in red.

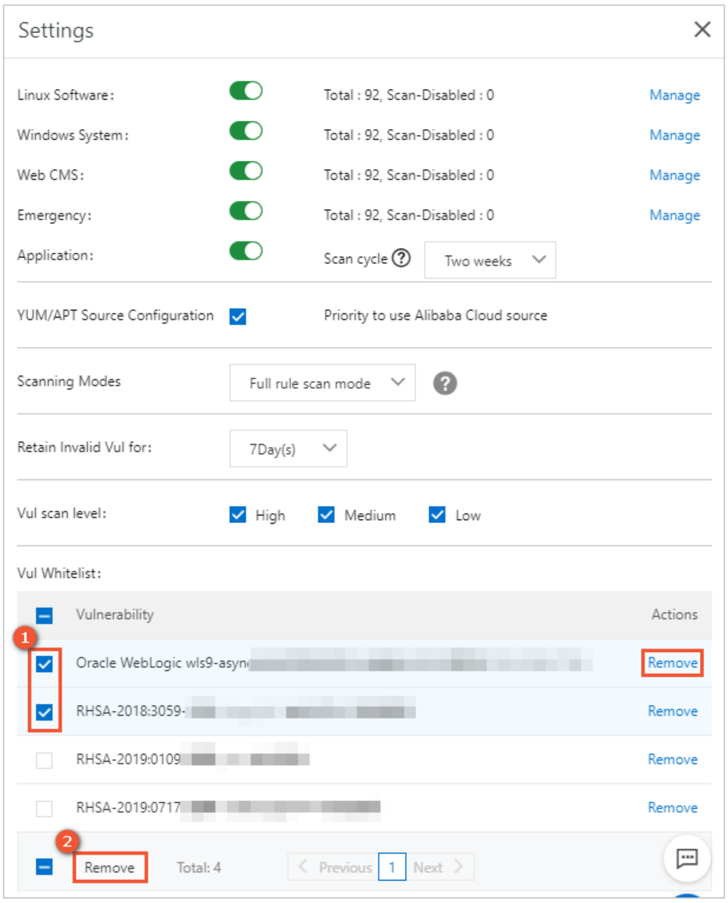
Note We recommend that you fix Web-CMS vulnerabilities at the earliest opportunity.

- **Handle the vulnerabilities detected by Cloud Firewall**
  Security Center uses the **Cloud firewall Supports Virtual patches** tag to indicate a vulnerability detected by Cloud Firewall. You can click the tag or **Protection** in the Actions column to go to the Cloud Firewall console to fix the vulnerability. For more information, see Vulnerability protection.
- **Add a vulnerability to the whitelist**
  On the **Web CMS** tab, you can select the vulnerability you want to add to the whitelist and click **Add to Whitelist**. After you add a vulnerability to the whitelist, Security Center no longer generates alerts on this vulnerability.



	Vulnerability	Affected Assets	Latest Scan Time	Actions
□	GET Request CSRF Vulnerability in PHPWind Task Center	1	Mar 30, 2021, 09:49:06	Fix
□	PHPCMS2008 "template" Cache Abuse Leads to Remote Code Execution Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:49:01	Fix Protection
□	WE7 Unserialized Data SQL Injection Vulnerability Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:57	Fix Protection
□	RCE Vulnerabilities Caused by sitename Field in WordPress Mail Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:53	Fix Protection
□	phpmyadmin-Core.php-checkPageValidity-vul Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:49	Fix Protection
□	DedeCMS Payment Plug-in SQL Injection Vulnerability Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:45	Fix Protection
□	FCKeditor Arbitrary File Upload Vulnerability Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:39	Fix Protection
□	ThinkPHP <5.0.24 Request.php Remote Code Execution Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:33	Fix Protection
☑	Joomla! Unauthorized User Creation Vulnerability (CVE-2016-8870)	1	Mar 30, 2021, 09:48:29	Fix
☑	ECShop SQL Injection Vulnerability Cloud firewall Supports Virtual patches	1	Mar 30, 2021, 09:48:22	Fix Protection

  The vulnerability that is added to the whitelist is removed from the vulnerability list on the **Web CMS** tab. You can click **Settings** in the upper-right corner of the page to view the vulnerability in the **Vul Whitelist** section.
  If you want Security Center to detect and generate alerts for a vulnerability that is added to the whitelist, select the vulnerability in the Vul Whitelist section in the **Settings** panel and click **Remove**.



Settings

Linux Software:	On	Total : 92, Scan-Disabled : 0	Manage
Windows System:	On	Total : 92, Scan-Disabled : 0	Manage
Web CMS:	On	Total : 92, Scan-Disabled : 0	Manage
Emergency:	On	Total : 92, Scan-Disabled : 0	Manage
Application:	On	Scan cycle ⓘ Two weeks	

YUM/APT Source Configuration ☑ Priority to use Alibaba Cloud source

Scanning Modes: Full rule scan mode

Retain Invalid Vul for: 7Day(s)

Vul scan level: ☑ High ☑ Medium ☑ Low

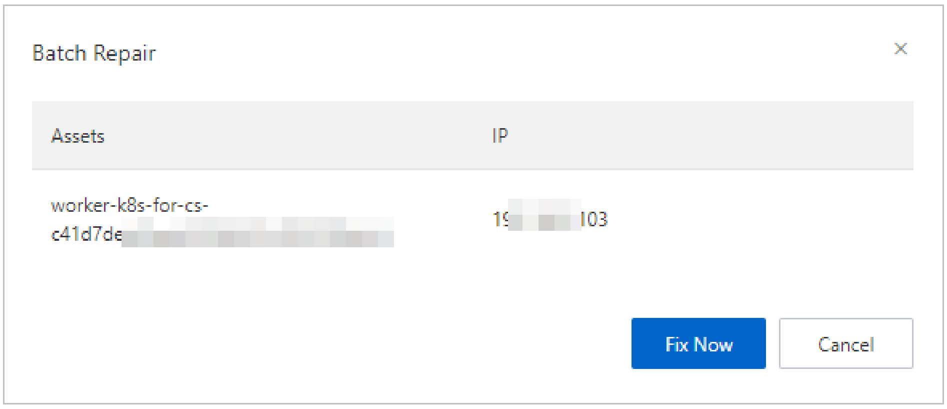
Vul Whitelist:

☐	Vulnerability	Actions
☑	Oracle WebLogic wls9-async[redacted]	Remove
☑	RHSA-2018:3059-[redacted]	Remove
☐	RHSA-2019:0109[redacted]	Remove
☐	RHSA-2019:0717[redacted]	Remove

Remove Total: 4 < Previous 1 Next >

- **Fix multiple vulnerabilities at a time**

  If you fix multiple vulnerabilities at a time, Security Center automatically identifies affected assets and fixes the vulnerabilities on these assets. On the **Web CMS** tab, you can select the vulnerabilities that you want to fix and click **Batch Repair**. In the **Batch Repair** dialog box, view the assets that are affected by the vulnerabilities and click **Fix Now**.



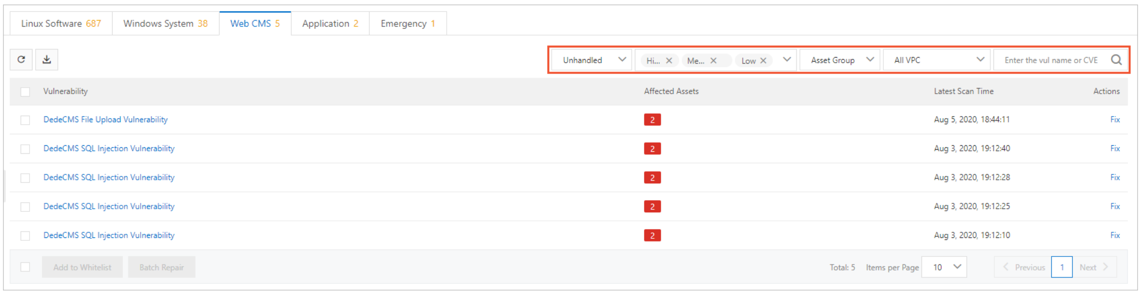
Batch Repair

Assets	IP
worker-k8s-for-cs-c41d7de[redacted]	1[redacted]03

> **Note** You can select the vulnerabilities only on the current page. A total of 10, 20, or 50 vulnerabilities can be displayed on each page. Therefore, you can fix a maximum of 50 vulnerabilities at a time.

- **Search for vulnerabilities**

On the **Web CMS** tab, you can search for vulnerabilities by severity level, asset group, vulnerability status, or vulnerability name. The severity level can be high, medium, or low. The vulnerability status can be handled or unhandled.



Linux Software 687 | Windows System 38 | Web CMS 5 | Application 2 | Emergency 1

Unhandled | Hi... × Me... × Low × | Asset Group | All VPC | Enter the vul name or CVE

□	Vulnerability	Affected Assets	Latest Scan Time	Actions
□	DedeCMS File Upload Vulnerability	2	Aug 5, 2020, 18:44:11	Fix
□	DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:40	Fix
□	DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:28	Fix
□	DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:25	Fix
□	DedeCMS SQL Injection Vulnerability	2	Aug 3, 2020, 19:12:10	Fix

□ Add to Whitelist | Batch Repair Total: 5 Items per Page 10 < Previous 1 Next >

Note

- **Export vulnerabilities**

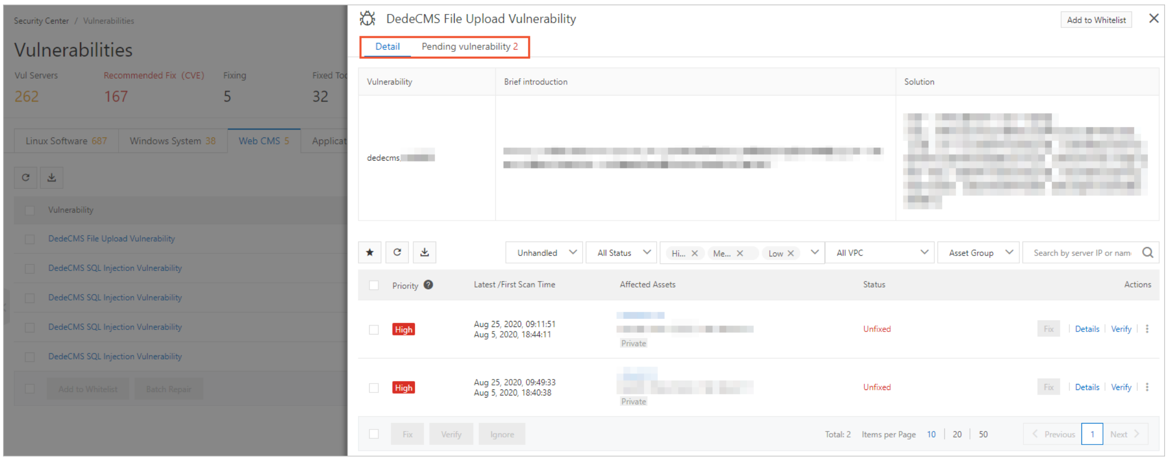
  On the **Web CMS** tab, you can click the ⤓ icon to export and save all detected vulnerabilities to your computer. The vulnerabilities are exported to an Excel file.

  Note The time that is required to export the vulnerabilities varies based on the size of vulnerability data.

Handle vulnerabilities

1.
2.
3.
4. In the **Vulnerability** column, click the name of the vulnerability that you want to handle, or click **Fix** in the **Actions** column of the vulnerability that you want to handle. The panel that shows the vulnerability details appears.

   You can view the details of the vulnerability, number of unhandled vulnerabilities, and information about affected assets.



Security Center / Vulnerabilities

Vulnerabilities

Vul Servers 262 | Recommended Fix (CVE) 167 | Fixing 5 | Fixed To 32

Linux Software 687 | Windows System 38 | Web CMS 5 | Applicat

□	Vulnerability
□	DedeCMS File Upload Vulnerability
□	DedeCMS SQL Injection Vulnerability
□	DedeCMS SQL Injection Vulnerability
□	DedeCMS SQL Injection Vulnerability
□	DedeCMS SQL Injection Vulnerability

□ Add to Whitelist | Batch Repair

DedeCMS File Upload Vulnerability Add to Whitelist ×

Detail | Pending vulnerability 2

Vulnerability	Brief introduction	Solution
dedecms [redacted]	[redacted]	[redacted]

Unhandled | All Status | Hi... × Me... × Low × | All VPC | Asset Group | Search by server IP or nam

□	Priority	Latest /First Scan Time	Affected Assets	Status	Actions
□	High	Aug 25, 2020, 09:11:51 Aug 5, 2020, 18:44:11	[redacted] Private	Unfixed	Fix | Details | Verify | ⋮
□	High	Aug 25, 2020, 09:49:33 Aug 5, 2020, 18:40:38	[redacted] Private	Unfixed	Fix | Details | Verify | ⋮

□ Fix | Verify | Ignore Total: 2 Items per Page 10 | 20 | 50 < Previous 1 Next >

5. In the panel, view and handle the vulnerability.

   You can perform the following operations:

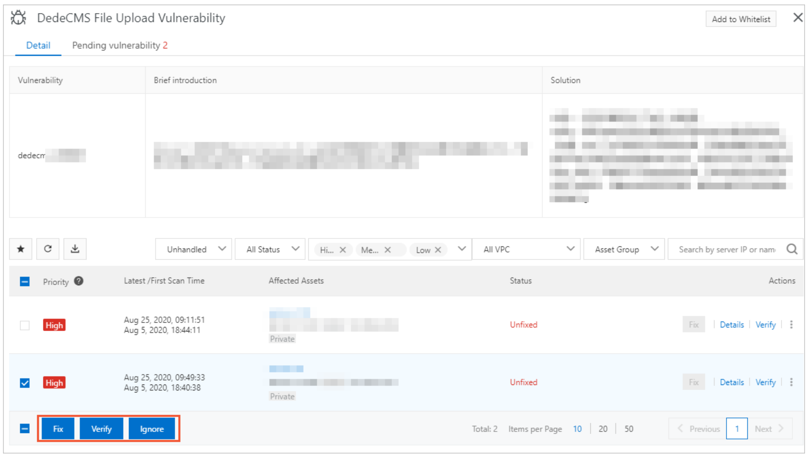
   - View vulnerability details

- **View vulnerability details**

  The panel displays all the affected assets and vulnerabilities associated with the vulnerability. You can analyze all the related vulnerabilities and handle multiple vulnerabilities at a time.

  - On the **Detail** tab, you can view the brief introduction and solution to this vulnerability.
  - On the **Pending vulnerability** tab, you can view the assets that are affected by this vulnerability.

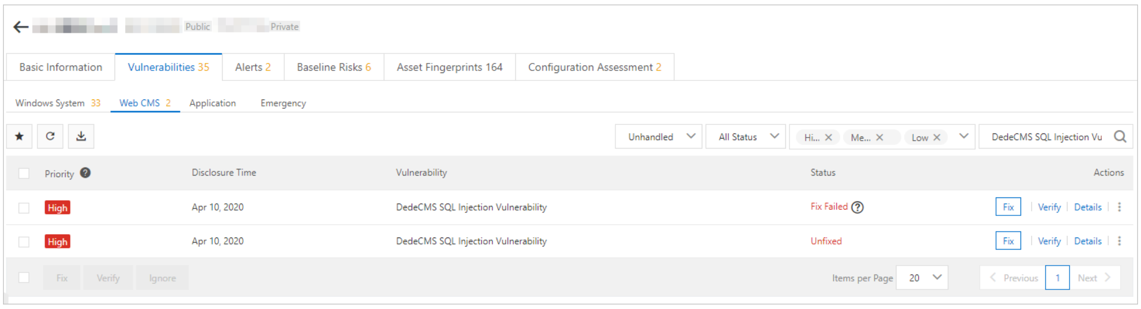
    You can view the assets affected by the vulnerability and the status of the vulnerability. You can fix or ignore a vulnerability. You can also verify a vulnerability fix or add a vulnerability to the whitelist.



Vulnerability	Brief introduction	Solution
dedecm		

Priority	Latest /First Scan Time	Affected Assets	Status	Actions
High	Aug 25, 2020, 09:11:51 Aug 5, 2020, 18:44:11	Private	Unfixed	Fix | Details | Verify
High	Aug 25, 2020, 09:49:33 Aug 5, 2020, 18:40:38	Private	Unfixed	Fix | Details | Verify

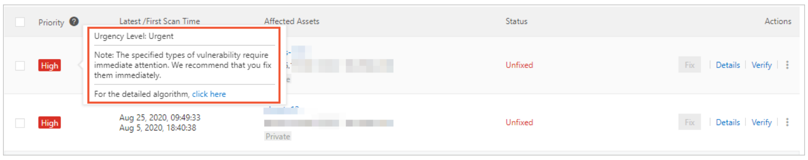
On the **Detail** tab, click an asset in the **Affected Assets** column to go to the **Vulnerabilities** tab of the **Assets** page. On this tab, view the information about all Web-CMS vulnerabilities associated with this asset.



Priority	Disclosure Time	Vulnerability	Status	Actions
High	Apr 10, 2020	DedeCMS SQL Injection Vulnerability	Fix Failed	Fix | Verify | Details
High	Apr 10, 2020	DedeCMS SQL Injection Vulnerability	Unfixed	Fix | Verify | Details

- **View vulnerability priorities**

  All Web-CMS vulnerabilities can cause serious damage. This is confirmed by Alibaba Cloud security engineers. Therefore, the priorities of detected Web-CMS vulnerabilities are **High** and marked in red.



Urgency Level: Urgent

Note: The specified types of vulnerability require immediate attention. We recommend that you fix them immediately.

For the detailed algorithm, click here

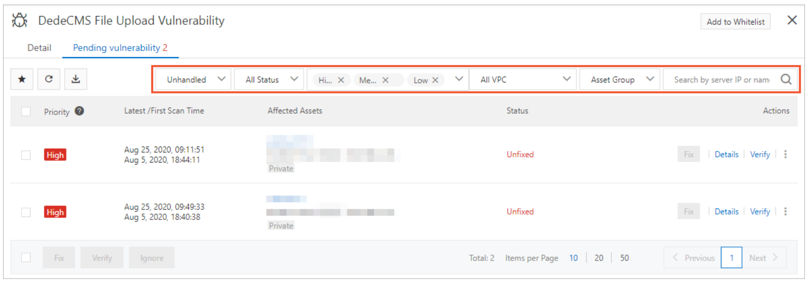
Priority	Latest /First Scan Time	Affected Assets	Status	Actions
High			Unfixed	Fix | Details | Verify
High	Aug 25, 2020, 09:49:33 Aug 5, 2020, 18:40:38	Private	Unfixed	Fix | Details | Verify

Note We recommend that you fix Web-CMS vulnerabilities at the earliest opportunity.

- **Search for vulnerabilities**

  On the Pending vulnerability tab, you can search for affected assets by vulnerability priority, VPC name, asset group, vulnerability status, server IP address, or server name. The vulnerability priority can be high, medium, or low. The vulnerability status can be handled or unhandled.

> **Note** If you search for affected assets by server IP address or name, fuzzy match is supported.

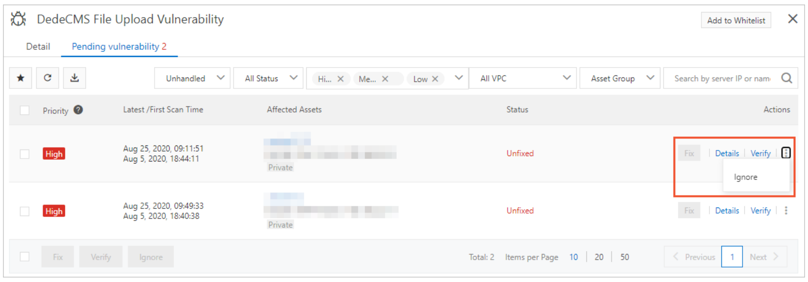


Priority	Latest /First Scan Time	Affected Assets	Status	Actions
High	Aug 25, 2020, 09:11:51 Aug 5, 2020, 18:44:11	[redacted] Private	Unfixed	Fix | Details | Verify
High	Aug 25, 2020, 09:49:33 Aug 5, 2020, 18:40:38	[redacted] Private	Unfixed	Fix | Details | Verify

> **Note** Fuzzy match is supported for vulnerability search by server IP address or name.

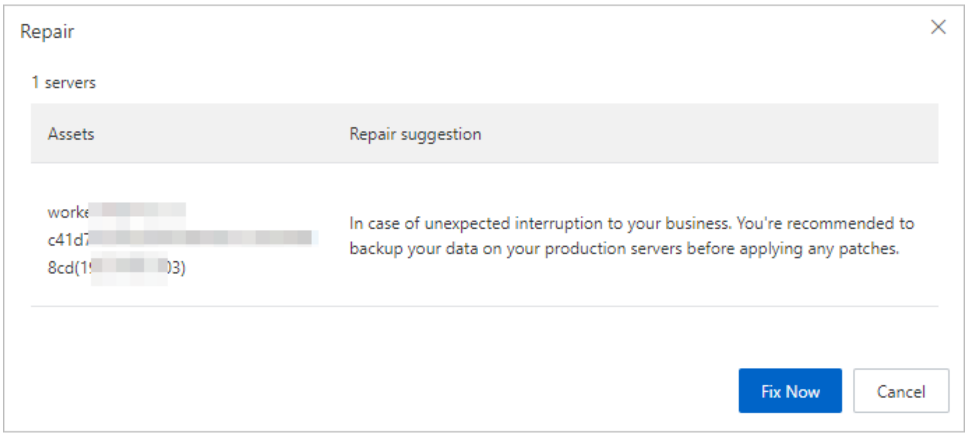
- View vulnerability status
  - **Handled**
    - Handled: The vulnerability is fixed.
    - Ignored: The vulnerability is **ignored**. Security Center no longer generates alerts on this vulnerability.
    - Invalid: The vulnerability cannot be detected. You may have already deleted the file that contains the vulnerability.
  - **Unhandled**
    - Unfixed: The vulnerability is not fixed.
    - Fixing: The vulnerability is being fixed.
    - Fix Failed: Security Center failed to fix the vulnerability. The file that contains the vulnerability may have been modified or does not exist.
    - Verifying: Security Center is checking whether the vulnerability is fixed.
- **Handle the vulnerabilities of the affected assets**

  You can fix or ignore a vulnerability. You can also verify a vulnerability fix or add a vulnerability to the whitelist.



Priority	Latest /First Scan Time	Affected Assets	Status	Actions
High	Aug 25, 2020, 09:11:51 Aug 5, 2020, 18:44:11	[redacted] Private	Unfixed	Fix | Details | Verify Ignore
High	Aug 25, 2020, 09:49:33 Aug 5, 2020, 18:40:38	[redacted] Private	Unfixed	Fix | Details | Verify

- **Fix vulnerabilities**
  Click **Fix** in the Actions column to fix one or more associated vulnerabilities at a time. In the **Repair** dialog box, click **Fix Now**.



Repair

1 servers

Assets	Repair suggestion
worke[redacted] c41d7[redacted] 8cd(1[redacted]03)	In case of unexpected interruption to your business. You're recommended to backup your data on your production servers before applying any patches.

> **Note** To prevent service interruptions, we recommend that you back up the data in your system before you fix the vulnerability.

- **Verify**: If you fix a vulnerability by using methods rather than Security Center, you must click Verify. After the verification, the status of the vulnerability is updated. If you fix a Web-CMS vulnerability by using Security Center, the fix immediately takes effect. You do not need to verify the fix.
- **Ignore a vulnerability**

  Find the vulnerability that you want to ignore, click the ⋮ icon in the **Actions** column, and then select **Ignore**. In the dialog box that appears, enter the description for the ignore operation and click **OK**. After a vulnerability is ignored, Security Center no longer generates alerts for the vulnerability.
  Search for **Handled** vulnerabilities, find the vulnerability that is ignored, and then click the vulnerability to go to the panel that shows the vulnerability details. In the panel, move the pointer over the ? icon in the Status column to view the description of the ignore operation.

> **Note** The state of this vulnerability changes to **Ignored**. If you want Security Center to generate alerts on an ignored vulnerability, find the vulnerability in the **Handled** vulnerability list and click **Unignore** in the panel.

- **Export affected assets**

  In the upper-left corner of the Pending vulnerability tab, click the ⤓ icon to export and save all affected assets to your computer. The exported file is in the Excel format.

> **Note** The time that is required to export the vulnerabilities varies based on the size of asset data.

Web-CMS vulnerabilities that can be detected

Type	Item
74CMS	Multiple SQL injection vulnerabilities in 74CMS
	Privilege escalation vulnerability in 74CMS
	SQL injection vulnerability in 74CMS
	Arbitrary file deletion vulnerability in 74CMS v4.1.15
	Arbitrary file read vulnerability in the latest version of 74CMS
DedeCMS	Variable overwrite vulnerability in DedeCMS
	Arbitrary file upload vulnerability in DedeCMS
	Reinstallation vulnerability in DedeCMS
	Injection vulnerability in DedeCMS
	File upload vulnerability in DedeCMS
	Password resetting vulnerability in DedeCMS
	Vulnerability of arbitrary user logon from the frontend caused by cookie leaks in DedeCMS
	SQL injection vulnerability caused by session variable overwrite in DedeCMS
	Vulnerability of arbitrary file upload at the backend in DedeCMS
	SQL injection vulnerability in DedeCMS
	Template SQL injection vulnerability in DedeCMS
	SQL injection vulnerability caused by cookie leaks in DedeCMS
	Payment plug-in injection vulnerability in DedeCMS
	Arbitrary file deletion by registered users in DedeCMS V5.7
	CSRF protection bypass vulnerability in DedeCMS V5.7
	Arbitrary file upload by common users in DedeCMS select_soft_post.php
	Arbitrary file upload vulnerability in DedeCMS V5.7 SP2 (CVE-2019-8362)
	Code execution vulnerability in Discuz
	MemCache + ssrf permission acquisition vulnerability (GetShell) in Discuz

Type	Item
Discuz	Backend SQL injection vulnerability in Discuz
	Arbitrary attachment download caused by privilege escalation vulnerabilities in Discuz
	Arbitrary file deletion vulnerability in Discuz
	Encrypted message forgery vulnerability caused by authcode function defects in Discuz
	Discuz!Command execution vulnerability in the backend database backup feature of Discuz
ECShop	Code injection vulnerability in ECShop
	Password retrieval vulnerability in ECShop
	Injection vulnerability in ECShop
	ECShop backdoor
	Arbitrary user logon vulnerability in ECShop
	Backend SQL injection vulnerability in ECShop
	SQL injection vulnerability in ECShop
	Vulnerability of overwriting variables in the ECShop installation directory at the backend
	Code execution caused by SQL injection vulnerabilities in ECShop
	Secondary injection vulnerability in ECShop
	Backend permission acquisition vulnerability in ECShop (GetShell)
	Backend file download vulnerability in ECShop 2.7.3
FCKEditor	Arbitrary file upload vulnerability in FCKeditor
Joomla!	Remote code execution (RCE) vulnerability caused by malformed deserialized packet injection in Joomla!
	Unauthorized user creation vulnerability in Joomla! (CVE-2016-8870)
	Core SQL injection vulnerability in Joomla! 3.7.0
	SQL injection vulnerability in Joomla!
	Injection vulnerability in PHPCMS
	AuthKey leak vulnerability in PHPCMS

Type	Item
PHPCMS	Wide byte injection vulnerability in PHPCMS v9
	Arbitrary file read vulnerability caused by frontend code injection in PHPCMS
	Permission acquisition vulnerability caused by some logic issues in PHPCMS (GetShell)
	AuthKey leak caused by AuthKey generation algorithm issues in PHPCMS
	SQL injection vulnerability in PHPCMS v9.6.2
	common.inc RCE vulnerability in PHPCMS 2008
	RCE vulnerability in template cache of PHPCMS 2008
phpMyAdmin	Deserialized injection vulnerability in phpMyAdmin
	CVE-2016-6617 SQL injection vulnerability in phpMyAdmin
	Permission acquisition vulnerability caused by checkPageValidity function defects in phpMyAdmin version 4.8.1 and earlier (GetShell)
	phpMyAdmin 4.8.5
PHPWind	GET request CSRF vulnerability in PHPWind v9 task center
	Permission acquisition vulnerability caused by MD5 padding vulnerabilities in PHPWind v9 (GetShell)
	Backend SQL injection vulnerability in PHPWind
	Cross-site scripting (XSS) injection into UBB tag attributes in PHPWind
ThinkPHP5	Medium-risk permission acquisition vulnerability caused by cache function design flaws in ThinkPHP 5.0.10-3.2.3 (GetShell)
	High-risk RCE vulnerability in ThinkPHP 5.0
	ThinkPHP 5.1.X <=5.1.30.RCE vulnerability in ThinkPHP 5.1.X (X less than or equal to 30)
	High-risk Request.php RCE vulnerability in versions earlier than ThinkPHP 5.0.24
	Arbitrary file upload vulnerability in WordPress
	IP address verification vulnerability in WordPress
	WP_Image_Editor_Imagick instruction injection vulnerability in WordPress

Type	Item
WordPress	XSS vulnerability in the bbPress plug-in of WordPress
	Mailpress RCE vulnerability in WordPress
	DOS vulnerability caused by arbitrary directory traversal in the backend plug-in update module of WordPress
	SQL injection vulnerability caused by arbitrary user logon to the backend plug-in of WordPress
	Username enumeration vulnerability in versions earlier than WordPress 4.7.1 (CVE-2017-5487)
	SQL injection vulnerability in WordPress
	XSS vulnerability in WordPress
	Content injection vulnerability in WordPress
	RCE vulnerabilities caused by the sitename field in WordPress Mail
	SQL injection vulnerability in the Catalogue plug-in of WordPress
	Arbitrary file deletion vulnerability in WordPress
	Permission acquisition vulnerability caused by multiple defects, such as Author permission path traversal in WordPress (GetShell)

1.6. View and handle application vulnerabilities

The application vulnerability detection feature can detect common application vulnerabilities. This topic describes how to view and handle application vulnerabilities.

Limits

- Security Center can detect application vulnerabilities, but it cannot fix the detected application vulnerabilities. You must manually fix the vulnerabilities on your servers by following **Suggestions** on the **Detail** tab.
- Security Center provides two modes to scan application vulnerabilities: **Web Scanner** and **Software Component Analysis**. The two modes have the following limits:
  - **Web Scanner**: scans only the servers that can access the Internet and have the Security Center agent installed. The servers can be Elastic Compute Service (ECS) instances or the servers that are not deployed on Alibaba Cloud.
  - **Software Component Analysis**: scans the servers that have the Security Center agent installed. The servers can be ECS instances or the servers that are not deployed on Alibaba Cloud.

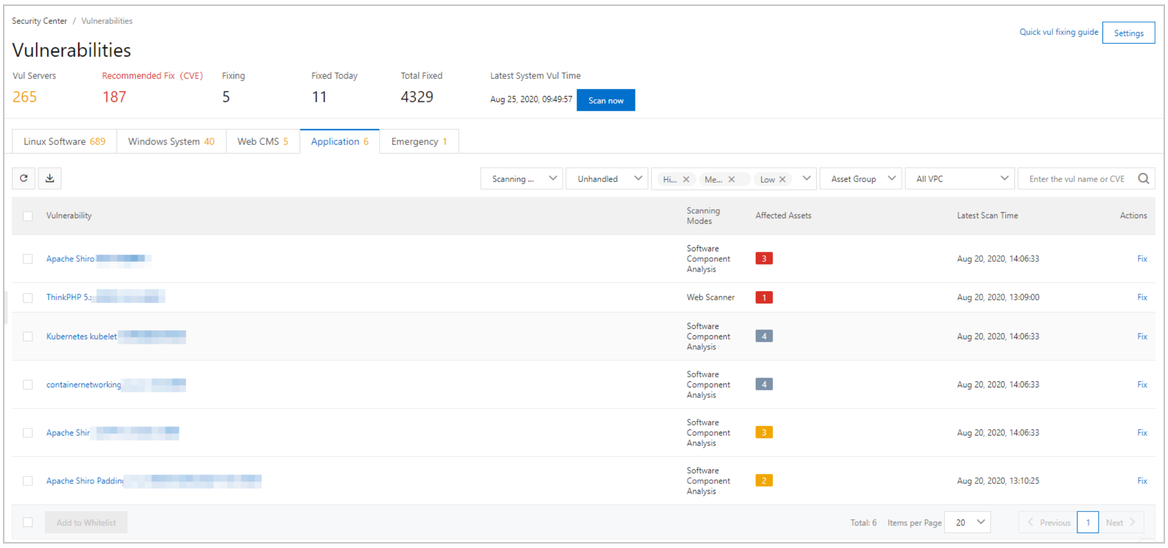
View the basic information about a vulnerability

1.

2.

3.

4. On the **Application** tab, view all the application vulnerabilities that are detected by Security Center.



Vulnerabilities

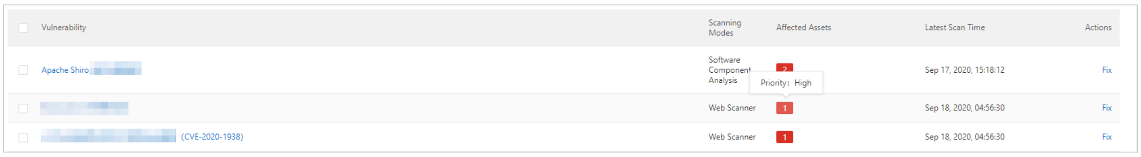
Vul Servers	Recommended Fix (CVE)	Fixing	Fixed Today	Total Fixed	Latest System Vul Time
265	187	5	11	4329	Aug 25, 2020, 09:49:57

Vulnerability	Scanning Modes	Affected Assets	Latest Scan Time	Actions
Apache Shiro [redacted]	Software Component Analysis	3	Aug 20, 2020, 14:06:33	Fix
ThinkPHP 5.[redacted]	Web Scanner	1	Aug 20, 2020, 13:09:00	Fix
Kubernetes kubelet [redacted]	Software Component Analysis	4	Aug 20, 2020, 14:06:33	Fix
containernetworking [redacted]	Software Component Analysis	4	Aug 20, 2020, 14:06:33	Fix
Apache Shir [redacted]	Software Component Analysis	3	Aug 20, 2020, 14:06:33	Fix
Apache Shiro Paddin [redacted]	Software Component Analysis	2	Aug 20, 2020, 13:10:25	Fix

Total: 6 Items per Page 20 1

You can perform the following operations on the tab:

- **Search for vulnerabilities**
  On the Application tab, you can search for vulnerabilities by severity level, vulnerability status, scan mode, asset group, virtual private cloud (VPC) name, or vulnerability name. The severity level can be high, medium, or low. The vulnerability status can be handled or unhandled. The scan mode can be web scanner or software component analysis. You can also search for vulnerabilities by server IP address or server name.
- **View vulnerabilities**
- **View vulnerability scan modes**
  Security Center scans for application vulnerabilities based on the following methods:
  - **Web Scanner:** inspects network traffic to detect vulnerabilities in your system. For example, you can use this method to scan for SSH weak passwords and remote command execution.
  - **Software Component Analysis:** identifies software versions to detect vulnerabilities in your system. For example, you can use this method to scan for vulnerabilities of Apache Shiro authorization and Kubernetes kubelet resource management.
- **View the priorities of vulnerabilities and the number of affected assets**
  The priorities of vulnerabilities are displayed in different colors in the Affected Assets column. The number in each row of the column indicates the total number of the assets affected by a vulnerability. The following list describes the relationship between colors and priorities:
  - Red: **High**
  - Orange: **Medium**
  - Gray: **Low**



Vulnerability	Scanning Modes	Affected Assets	Latest Scan Time	Actions
Apache Shiro [redacted]	Software Component Analysis	2	Sep 17, 2020, 15:18:12	Fix
[redacted]	Web Scanner	1	Sep 18, 2020, 04:56:30	Fix
[redacted] (CVE-2020-1938)	Web Scanner	1	Sep 18, 2020, 04:56:30	Fix

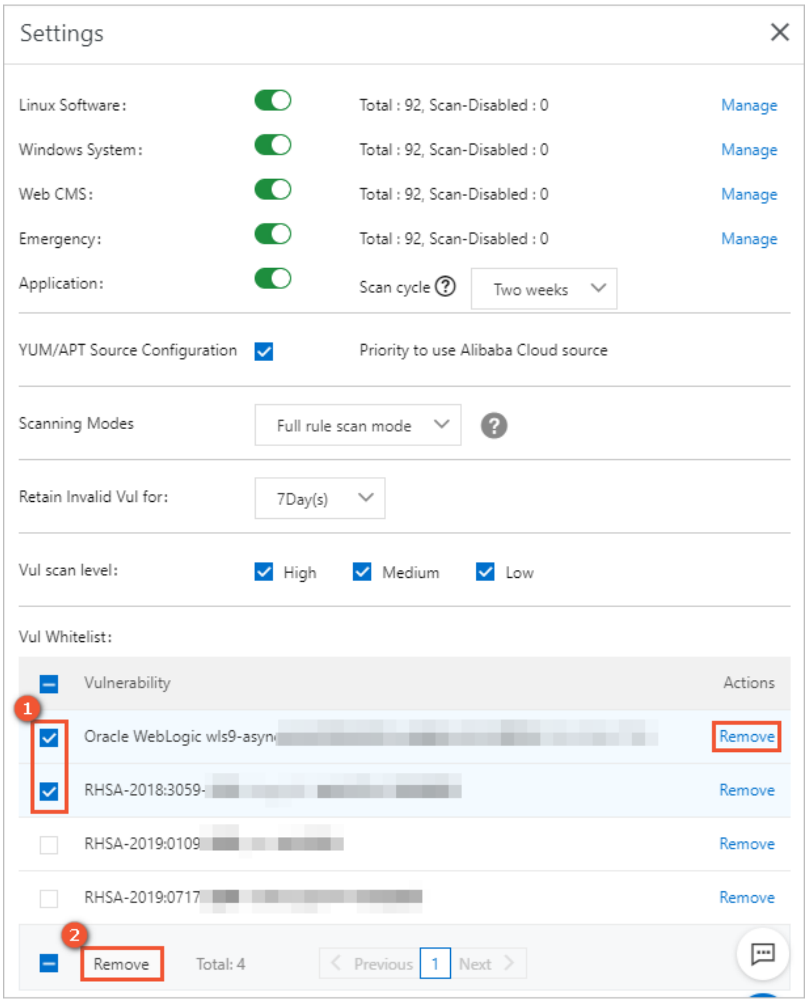
> Note We recommend that you fix the vulnerabilities that have the **High** priority at the earliest opportunity.

- **Add vulnerabilities to the whitelist**

  On the **Application** tab, you can select one or more vulnerabilities and click **Add to Whitelist** to add them to the whitelist. Security Center no longer generates alerts on the vulnerabilities that are added to the whitelist.

  Vulnerabilities that are added to the whitelist are not displayed in the vulnerability list on the **Application** tab. If you want to view these vulnerabilities, you can click **Settings** in the upper-right corner of the Vulnerabilities page and find the vulnerabilities in the **Vul Whitelist** section.

  If you want Security Center to detect and generate alerts for a vulnerability that is added to the whitelist, select the vulnerability in the Vul Whitelist section in the **Settings** panel and click **Remove**.



Settings

Linux Software:	●	Total : 92, Scan-Disabled : 0	Manage
Windows System:	●	Total : 92, Scan-Disabled : 0	Manage
Web CMS:	●	Total : 92, Scan-Disabled : 0	Manage
Emergency:	●	Total : 92, Scan-Disabled : 0	Manage
Application:	●	Scan cycle ? Two weeks	

YUM/APT Source Configuration ☑ Priority to use Alibaba Cloud source

Scanning Modes: Full rule scan mode

Retain Invalid Vul for: 7Day(s)

Vul scan level: ☑ High ☑ Medium ☑ Low

Vul Whitelist:

	Vulnerability	Actions
☑	Oracle WebLogic wls9-asyn[redacted]	Remove
☑	RHSA-2018:3059-[redacted]	Remove
□	RHSA-2019:0109[redacted]	Remove
□	RHSA-2019:0717[redacted]	Remove

- **Export vulnerabilities**

  On the **Application** tab, you can click the ⤓ icon to export and save all detected vulnerabilities to your computer. The vulnerabilities are exported to an Excel file.

> Note The time that is required to export the vulnerabilities varies based on the size of vulnerability data.

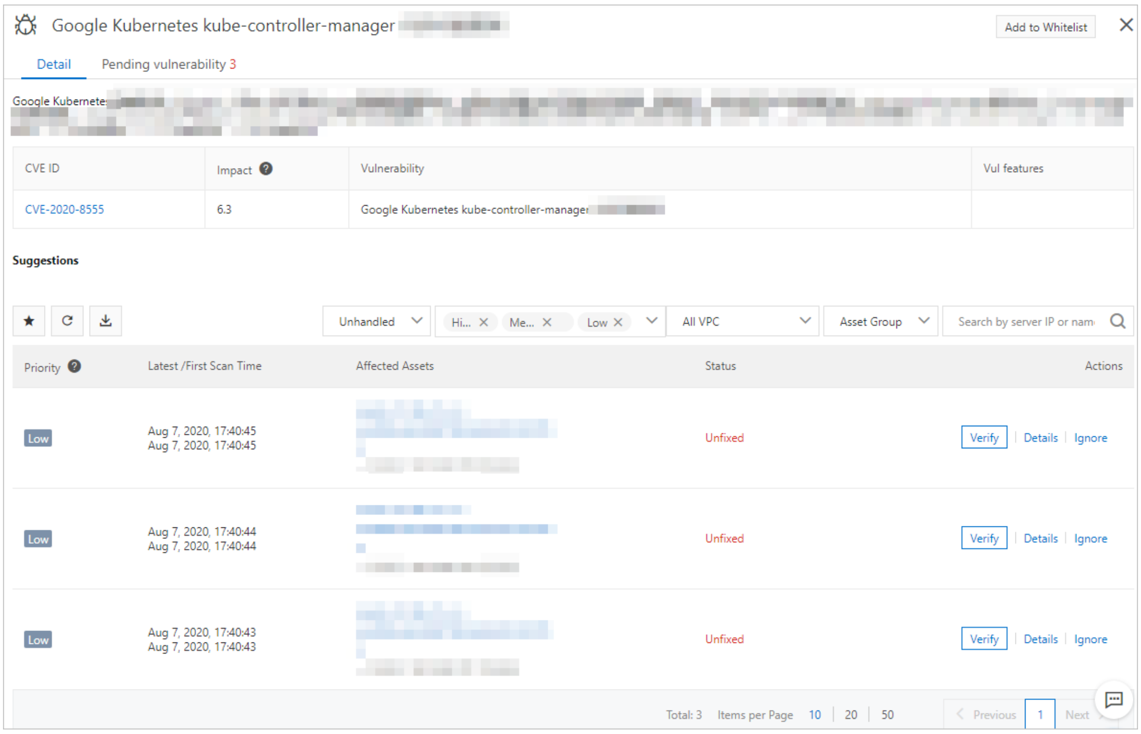
View vulnerability details and handle vulnerabilities

Note

1.
2.
3.
4. In the **Vulnerability** column, click the name of the vulnerability that you want to handle, or click **Fix** in the **Actions** column of the vulnerability that you want to handle to go to the panel that shows the vulnerability details.
5. In the panel, view and handle the vulnerability.

   You can perform the following operations:

   - **View vulnerability details**
     The panel displays all the affected assets and vulnerabilities associated with the vulnerability. You can analyze and handle multiple vulnerabilities at a time. You can view the following information:
     - On the Detail tab, you can view the associated vulnerabilities, descriptions, impacts, and characteristics.
     - On the **Pending vulnerability** tab, you can view the assets that are affected by this vulnerability.
       You can view the assets affected by the vulnerability and the status of the vulnerability. You can also verify a vulnerability fix, add a vulnerability to the whitelist, ignore a vulnerability, or restore an ignored vulnerability.



Google Kubernetes kube-controller-manager [redacted]

Google Kubernete [redacted]

CVE ID	Impact	Vulnerability	Vul features
CVE-2020-8555	6.3	Google Kubernetes kube-controller-manager [redacted]	

Suggestions

Priority	Latest /First Scan Time	Affected Assets	Status	Actions
Low	Aug 7, 2020, 17:40:45 Aug 7, 2020, 17:40:45	[redacted]	Unfixed	Verify | Details | Ignore
Low	Aug 7, 2020, 17:40:44 Aug 7, 2020, 17:40:44	[redacted]	Unfixed	Verify | Details | Ignore
Low	Aug 7, 2020, 17:40:43 Aug 7, 2020, 17:40:43	[redacted]	Unfixed	Verify | Details | Ignore

Click an asset in the **Affected Assets** column to go to the **Vulnerabilities** tab of the **Assets** page. Then, click the **Application** tab to view the information about all application vulnerabilities associated with this asset.

- **View the details about the Alibaba Cloud vulnerability library**
  On the **Detail** tab, find the vulnerability that you want to view and click **CVE ID** to go to the Alibaba Cloud vulnerability library. On the page that appears, view details about the vulnerability, including the vulnerability description, basic information, and solution.
- **View vulnerability status**
  The status of a vulnerability can be Handled or Unhandled.
  - **Handled**
    - Handled: The vulnerability is fixed.
    - Ignored: The vulnerability is **ignored**. Security Center no longer generates alerts on this vulnerability.
  - **Unhandled**
    - **Unfixed**: The vulnerability is to be fixed.
    - Verifying: After you start the verification, the state of the vulnerability changes to Verifying.

  > ⓘ **Note** By default, all the **unhandled** vulnerabilities are displayed in the application vulnerability list.
- **Verify vulnerability fixes**
  After you manually fix a vulnerability based on the **Suggestions** that are displayed on the **Detail** tab, click **Verify** to check whether the vulnerability is fixed. Find the vulnerability for which you want to verify the fix and click **Verify** in the Actions column.
  After you click Verify, the state of the vulnerability changes to **Verifying**. It takes several seconds to verify the vulnerability fix.
  The following list shows the two possible results:
  - Verification succeeded: The state of the vulnerability changes to **Fixed**. You can view the vulnerability in the **Handled** vulnerability list.
  - Verification failed: The state of the vulnerability changes to **Unfixed**. This indicates that the vulnerability has not been fixed. We recommend that you troubleshoot the issue and handle the vulnerability at the earliest opportunity.
- **Ignore vulnerabilities**
  If you do not want Security Center to generate alerts on some vulnerabilities, you can ignore these vulnerabilities. Select the vulnerability that you want to ignore and click **Ignore** in the Actions column. Security Center no longer generates alerts on this vulnerability.

  > ⓘ **Note** The state of this vulnerability changes to **Ignored**. If you want Security Center to generate alerts on an ignored vulnerability, find the vulnerability in the **Handled** vulnerability list and click **Unignore** in the panel.
- **Handle the vulnerabilities detected by Cloud Firewall**
  Security Center uses the **Cloud firewall Supports Virtual patches** tag to indicate a vulnerability detected by Cloud Firewall. You can click the tag or **Protection** in the Actions column to go to the Cloud Firewall console to fix the vulnerability. For more information, see Vulnerability protection.

Application vulnerabilities that can be detected

Vulnerability type	Check item
Weak passwords in system services	OpenSSH services
	MySQL database services
	Microsoft SQL Server (MSSQL) database services
	MongoDB database services
	FTP, VSFTP, and ProFTPD services
	Memcache cache services
	Redis caching services
	Subversion control services
	Server Message Block (SMB) file sharing services
	Simple Mail Transfer Protocol (SMTP) email delivery services
	Post Office Protocol 3 (POP3) email reception services
	Internet Message Access Protocol (IMAP) email management services
Vulnerabilities in system services	OpenSSL heartbleed vulnerabilities
	SMB • Samba • Brute-force attacks against weak passwords
	RSYNC • Anonymous access to sensitive data • Brute-force attacks against password-based authentication
	Brute-force attacks against VNC passwords
	Brute-force attacks against pcAnywhere passwords
	Brute-force attacks against Redis passwords
	phpMyAdmin weak passwords
	Tomcat console weak passwords
	Apache Struts 2 remote command execution vulnerabilities
	Apache Struts 2 remote command execution vulnerability (S2-046)
	Apache Struts 2 remote command execution vulnerability (S2-057)

Vulnerability type	Check item
Vulnerabilities in application services	Arbitrary file uploads in ActiveMQ (CVE-2016-3088)
	Arbitrary file reads in Confluence
	CouchDB Query Server remote command execution
	Discuz!Brute-force attacks against administrator weak passwords
	Unauthorized access to Docker
	Remote code execution in Drupal Drupalgeddon 2 (CVE-2018-7600)
	ECshop code execution vulnerabilities in logon endpoints
	Unauthorized access to Elasticsearch
	Elasticsearch MvelRCE CVE-2014-31
	Elasticsearch Groovy RCE CVE-2015-1427
	Expression Language (EL) Injection in Weaver OA
	Unauthorized access to Hadoop YARN ResourceManager
	Path traversal in JavaServer Faces 2
	Java deserialization in JBoss EJBInvokerServlet
	Anonymous access to Jenkins Manage (CVE-2018-1999001 and CVE-2018-1999002)
	Unauthorized access to Jenkins
	Jenkins Script Security Plugin RCE
	Unauthorized access to Kubernetes
	SQL injection vulnerabilities in the MetInfo getPassword interface
	SQL injection vulnerabilities in the MetInfo logon interface
	Arbitrary file uploads in PHPCMS 9.6
	PHP-CGI remote code execution vulnerabilities
	Actuator unauth RCE
	ThinkPHP_RCE_20190111
	Server-side request forgery (SSRF) in WebLogic UDDI Explorer
	SSRF in WordPress xmlrpc.php

Vulnerability type	Check item
	Brute-force attacks against the Zabbix web console
	OpenSSL heartbleed detection
	Unauthorized access to the WEB-INF directory in Apache Tomcat

1.7. View and handle urgent vulnerabilities

Security Center detects high-risk urgent vulnerabilities that are recently exposed on the Internet. You can check whether your assets are affected by these vulnerabilities at the earliest opportunity. This topic describes how to view and handle urgent vulnerabilities.

Context

The feature of urgent vulnerability detection provides the following benefits:

- Allows you to specify vulnerability severities before detection.
- Sorts urgent vulnerabilities by disclosure time.
- Detects urgent vulnerabilities and shows the detection progress.
- Generates alerts for urgent vulnerabilities and shows the details of affected assets and alerted vulnerabilities in real time.
- Shows the priorities to fix urgent vulnerabilities and provides suggestions on vulnerability fixes.
- Checks whether an urgent vulnerability is fixed.

> **Note** Security Center detects urgent vulnerabilities and provides suggestions on vulnerability fixes. However, it does not allow you to fix the detected urgent vulnerabilities with a few clicks. You must manually fix an **urgent vulnerability** on the affected servers based on **Suggestions** in the panel that shows the vulnerability details.

Limits

Security Center detects urgent vulnerabilities only on Alibaba Cloud Elastic Compute Service (ECS) instances. Security Center cannot detect urgent vulnerabilities on the servers that are not deployed on Alibaba Cloud or the servers in data centers.

Procedure

1.
2.
3.
4. On the **Emergency** tab, view both the historical and recent urgent vulnerabilities. Check whether your assets are affected by these vulnerabilities.

   You can perform the following operations:

   - **Detect vulnerabilities**
     Security Center allows you to detect urgent vulnerabilities by using the following methods:

  - **Detect all vulnerabilities with a few clicks**
    Click **Scan now** below **Latest System Vul Time**. In the **Scan for Vulnerabilities** dialog box, select **Emergency** and click **OK**. Then, Security Center scans all your servers to detect urgent vulnerabilities. For more information, see Use the quick scan feature.
  - **Immediately detect a single vulnerability**
    In the vulnerability list, find the vulnerability that you want to detect and click **Check Now** in the Actions column. After you click Check Now, the detection progress is updated in real time.
  - **Perform periodic detection** (Periodic detection is supported only by the , , and editions.)
    In the **Settings** panel, configure Emergency vul(s) Scan Cycle. By default, the detection period for urgent vulnerabilities is *00:00:00* to *07:00:00*. You can set Emergency vul(s) Scan Cycle to 3 Days, One week, Two weeks, or Stop. For more information, see Configure vulnerability settings.

    > Note If your servers are deployed in a private network or urgent vulnerability detection is not required, you can set Emergency vul(s) Scan Cycle to Stop. However, your servers may be attacked in various ways. We recommend that you set Emergency vul(s) Scan Cycle to a value other than Stop. This way, Security Center detects urgent vulnerabilities on your servers in a timely manner.

  If a vulnerability is detected, the number of affected assets is displayed and highlighted in red in the **Risks** column of the vulnerability. You can click the name of the vulnerability to go to the panel that displays the vulnerability details. In the panel, you can view the vulnerability details and handle the vulnerability.

  > Note A vulnerability for which you never perform a scan task is displayed as **Uninspected** in the **Risks** column. If you never perform quick scan tasks or click **Check Now** in the **Actions** column, all urgent vulnerabilities are displayed as **Uninspected** in the **Risks** column. Security Center discloses high-risk urgent vulnerabilities that are exposed on the Internet but does not automatically detect these vulnerabilities. We recommend that you regularly check the urgent vulnerability list and specify the period for automatic detection or manually scan for urgent vulnerabilities.

- **Search for vulnerabilities**
  On the **Emergency** tab, you can search for vulnerabilities by detection mode, risk status, or vulnerability name. The detection mode can be Version or Network Scan. The risk status can be Risk or No risk.
  The following list describes the detection modes:
  - **Version**: Security Center collects information about software versions to detect and analyze vulnerabilities on your assets in a private network.
  - **Network Scan**: Security Center uses web scanners to detect vulnerabilities on your assets in the Internet. No manual configurations are required.
- **Export vulnerabilities**

  On the **Emergency** tab, you can click the ⤓ icon to export and save all urgent vulnerabilities that are detected on your assets to your computer.

  > Notice If no urgent vulnerabilities are detected on your assets, the export icon is dimmed.

- **View the vulnerability status of affected assets**

Category	Status	Description
Handled	Handled	The vulnerability is fixed.
	Fix failed	Security Center failed to fix the vulnerability. The file that contains the vulnerability may have been modified or does not exist.
	Ignored	The vulnerability is **ignored**. Security Center no longer generates alerts for this vulnerability.
	Invalid	The vulnerability has not been detected in the last seven days.
Unhandled	Unfixed	The vulnerability is not fixed.
	Verifying	After you manually fix a vulnerability, you can click **Verify** in the **Actions** column to check whether the vulnerability is fixed. After you click Verify, the status of the vulnerability changes to **Verifying** from **Unfixed**.

- **View the priorities to fix urgent vulnerabilities**
  Priorities to fix vulnerabilities are classified into high, medium, and low based on vulnerability severities, time when vulnerabilities are detected, and server status.

  Note We recommend that you fix vulnerabilities that have the **High** priority at the earliest opportunity.

- **Handle urgent vulnerabilities**
  Security Center detects urgent vulnerabilities and provides suggestions on vulnerability fixes. However, it does not allow you to fix the detected urgent vulnerabilities with a few clicks. You must manually fix an **urgent vulnerability** on the affected servers based on **Suggestions** in the panel that shows the vulnerability details.
  You can perform the following operations:

  - View **Suggestions** in the panel that displays the vulnerability details and manually fix the vulnerability on the affected servers.
  - **Verify**: Check whether the vulnerability is fixed.
  - **Ignore**: Ignore the vulnerability. Security Center no longer generates alerts for the vulnerability.

    Note The state of this vulnerability changes to **Ignored**. If you want Security Center to generate alerts on an ignored vulnerability, find the vulnerability in the **Handled** vulnerability list and click **Unignore** in the panel.

- **Handle the vulnerabilities detected by Cloud Firewall**
  Security Center uses the **Cloud firewall Supports Virtual patches** tag to indicate a vulnerability detected by Cloud Firewall. You can click the tag or **Protection** in the Actions column to go to the Cloud Firewall console to fix the vulnerability. For more information, see Vulnerability protection.

References

Why are the results different when Security Center scans multiple times for fastjson urgent vulnerabilities?

How often does Security Center detect vulnerabilities?

What are the differences between baselines and vulnerabilities?

What do I do if I cannot enable the vulnerability detection feature for a server on the Assets page?

1.8. View and handle container image vulnerabilities

Security Center can detect container image vulnerabilities. This helps you detect high-risk system and application vulnerabilities to ensure the security and reliability of container images. This topic describes how to view and handle container image vulnerabilities.

Context

Before you can view and handle container image vulnerabilities, you must enable container image scan. Container image scan is a value-added feature of Security Center and must be separately purchased. Only users of the ,, , and editions can purchase container image scan.

Scan for container image vulnerabilities

Scan images

View container image vulnerabilities

View image system vulnerabilities

Fix container image vulnerabilities

You cannot fix container image vulnerabilities with a few clicks. To fix container image vulnerabilities, you must perform operations on container images based on the detection results of image system vulnerabilities.

> **Note** We recommend that you handle vulnerabilities in container images at the earliest opportunity based on the information provided by Security Center. The information includes fixing commands, impact descriptions, and paths to malicious files.

After you fix container image vulnerabilities, you must perform a quick scan task on the **Image Security** page. Then, you can view the latest status of the vulnerabilities and check whether the vulnerabilities are fixed.

1.9. Configure vulnerability settings

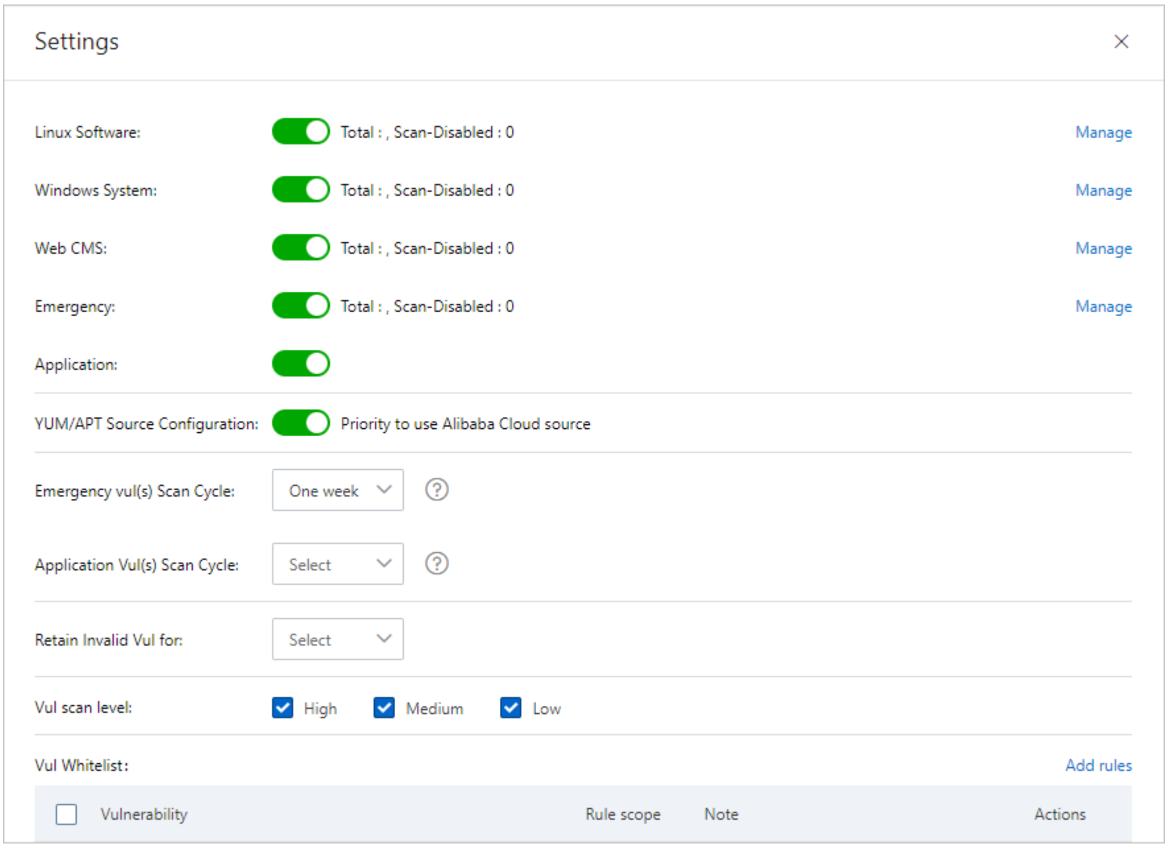
Security Center allows you to configure vulnerability settings. You can enable or disable automatic scan for each type of vulnerabilities, and enable vulnerability scan for specific servers. You can also specify the scan cycle, specify the number of days after which a detected vulnerability is automatically deleted, and remove vulnerabilities from the whitelist. This topic describes how to configure vulnerability settings.

Context

You can select multiple vulnerabilities from the list of Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, or application vulnerabilities. Then, you can add the selected vulnerabilities to the whitelist at a time. After you add vulnerabilities to the whitelist, Security Center no longer detects these vulnerabilities. You can also remove vulnerabilities from the whitelist in the **Settings** panel based on your business requirements.

Procedure

1.
2.
3.
4. In the **Settings** panel, configure the parameters based on your business requirements.



Settings ×

Linux Software: Total : , Scan-Disabled : 0 Manage

Windows System: Total : , Scan-Disabled : 0 Manage

Web CMS: Total : , Scan-Disabled : 0 Manage

Emergency: Total : , Scan-Disabled : 0 Manage

Application:

YUM/APT Source Configuration: Priority to use Alibaba Cloud source

Emergency vul(s) Scan Cycle: One week

Application Vul(s) Scan Cycle: Select

Retain Invalid Vul for: Select

Vul scan level: ☑ High ☑ Medium ☑ Low

Vul Whitelist: Add rules

□ Vulnerability	Rule scope	Note	Actions

The following table describes the parameters.

Parameter	Description
Linux Software	Turn on or turn off the switch to enable or disable the scan for Linux software vulnerabilities. After you turn on the switch, you can click **Manage** on the right to add or remove servers that you want to scan for Linux software vulnerabilities.
Windows System	Turn on or turn off the switch to enable or disable the scan for Windows system vulnerabilities. After you turn on the switch, you can click **Manage** on the right to add or remove servers that you want to scan for Windows system vulnerabilities.

Parameter	Description
Web CMS	Turn on or turn off the switch to enable or disable the scan for Web-CMS vulnerabilities. After you turn on the switch, you can click **Manage** on the right to add or remove servers that you want to scan for Web-CMS vulnerabilities.
Emergency	Turn on or turn off the switch to enable or disable the scan for urgent vulnerabilities. After you turn on the switch, you can click **Manage** on the right to add or remove servers that you want to scan for urgent vulnerabilities.
Application	Turn on or turn off the switch to enable or disable the scan for application vulnerabilities.
YUM/APT Source Configuration	Turn on or turn off the switch to specify whether to preferentially use YUM or APT sources of Alibaba Cloud to fix vulnerabilities. **Note** Before you fix a Linux software vulnerability, you must specify a valid YUM or APT source. If you specify an invalid YUM or APT source, the vulnerability may fail to be fixed. After you turn on the switch, Security Center automatically selects a YUM or APT source of Alibaba Cloud. This improves the success rate of vulnerability fixing. We recommend that you turn on **YUM/APT Source Configuration**.
Emergency vul(s) Scan Cycle	Specify the scan cycle for urgent vulnerabilities. Valid values: ○ 3 Days ○ One week ○ Two weeks ○ Stop **Note** ○ Only users of the , , and editions of Security Center can specify the **Emergency vul(s) Scan Cycle** parameter. By default, the scan period for urgent vulnerabilities is *00:00:00* to *07:00:00*. ○ If your servers are deployed in a private network or urgent vulnerability detection is not required, you can set **Emergency vul(s) Scan Cycle** to **Stop**. ○ Your servers may be attacked in various ways. We recommend that you set Emergency vul(s) Scan Cycle to a value other than Stop. This way, Security Center detects urgent vulnerabilities on your servers in a timely manner.

Parameter	Description
Application Vul(s) Scan Cycle	Specify the scan cycle for application vulnerabilities. Valid values: ○ 3 Days ○ One week ○ Two weeks ? **Note** Only users of the and editions of Security Center can specify the **Application Vul(s) Scan Cycle** parameter. By default, the scan period for application vulnerabilities is *00:00:00* to *07:00:00*.
Retain Invalid Vul for	Specify the number of days after which a detected vulnerability is automatically deleted. Valid values: ○ 7Day(s) ○ 30Day(s) ○ 90Day(s) ? **Note** If you do not handle a detected vulnerability and the vulnerability is no longer detected in multiple subsequent detection, the vulnerability is automatically removed from the Vulnerabilities page after the specified number of days. If vulnerabilities of the same type are detected, Security Center still generates alerts.
Vul scan level	Specify priorities for the vulnerabilities that Security Center detects. Valid values: ○ High ○ Medium ○ Low ? **Note** Security Center detects and displays only vulnerabilities that have the priorities specified by the **Vul scan level** parameter. If you set this parameter to **High** and **Medium**, Security Center detects only vulnerabilities that have **High** and **Medium** priorities. On the **Vulnerabilities** page, only vulnerabilities that have **High** and **Medium** priorities are displayed.

Parameter	Description
Vul Whitelist	Manage the vulnerability whitelist. You can perform the following operations: ○ **Add whitelist rules**: Click **Add rules** on the right. In the **AddVulnerability rule** panel, configure a whitelist rule based on a specific type of vulnerabilities. ○ **Edit whitelist rules**: Click **Edit** on the right of the vulnerability that is added to a whitelist rule. In the panel that appears, modify the **Rule scope** and **Note** parameters. ○ **Remove vulnerabilities from the whitelist**: Click **Delete** on the right of a vulnerability to remove the vulnerability from the whitelist. After you remove the vulnerability from the whitelist, Security Center can detect the vulnerability and generate alerts for the vulnerability.

After the vulnerability settings are configured, Security Center detects vulnerabilities on your servers based on the configurations.

Related information

- How often does Security Center detect vulnerabilities?
- What are the differences between baselines and vulnerabilities?
- What do I do if I cannot enable the vulnerability detection feature for a server on the Assets page?

1.10. Fix software vulnerabilities

This topic provides effective and reliable solutions to software vulnerabilities.

> ? **Note** The solutions provided in this topic can be used to fix vulnerabilities detected in operating systems, network devices, databases, and middleware on servers.

Procedure for fixing software vulnerabilities

Expertise on software security is required to fix software vulnerabilities on your servers. You must perform the following steps to fix software vulnerabilities:

Before the fix

- Check all assets on the server and log on to Security Center to check the vulnerabilities on the server.
- Determine the vulnerabilities that need to be fixed. You can fix vulnerabilities at separate times based on your business requirements. For example, you can select vulnerabilities to be fixed based on the business status, server resource usage, and impacts caused by vulnerability fixes.
- Upload vulnerability patches to the staging environment, test the compatibility and security of these patches, and then generate a test report. A test report must include the vulnerability fix result, fix duration, patch compatibility, and impacts caused by the vulnerability fix.
- Use the backup and recovery system to back up the data on the server in case of exceptions. For example, you can use the snapshot feature of ECS to create a snapshot of the ECS instance.

During the fix

- Upload vulnerability patches to the server and use the patches to fix vulnerabilities. This task requires a minimum of two administrators. One administrator is responsible for vulnerability fixes and the other one is responsible for recording the operations. Exercise caution when you fix vulnerabilities.

- Follow the system vulnerability list to upgrade the system and fix vulnerabilities.

After the fix

- Validate the vulnerability fixes on the server. Make sure that the vulnerabilities are fixed and that no exception occurs on the server.
- Generate a vulnerability fix report based on the entire vulnerability fix process and archive the relevant documents.

Risk prevention

To make sure that the server runs properly during the vulnerability fix process and minimize the possibility of exceptions, perform the following operations:

- **Develop a vulnerability fix plan**
  Research the operating system and applications of the server and develop an applicable plan. The feasibility of the plan must be discussed and verified in a staging environment. Make sure all operations in the vulnerability fix plan are performed and do not have negative impacts on the server.
- **Test the vulnerability fix plan**
  You must use a staging environment to verify the feasibility of your vulnerability fix plan. Make sure that the plan does not have negative impacts on the online business system to be fixed.
  Requirements for the staging environment:
  - The operating system and database system in the staging environment must be the same as those in the online business system.
  - The application system in the staging environment must be the same as that in the online business system.
  - We recommend that you use the last full backup of the online business system as the test data.
- **Back up the business system**
  Back up the entire business system, including the operating system, applications, and data. Then, check whether the backup data can be used to restore the system. If your system encounters an error or data loss, the system backup is used to restore the system. This ensures business stability. We recommend that you allow Security Center to automatically create snapshots to quickly back up your business system before you fix vulnerabilities.

> ? **Note** Security Center automatically creates a system snapshot of your server only if the vulnerability to be fixed is a Linux software vulnerability or a Windows system vulnerability.

1.11. Troubleshoot vulnerability fix failures

This topic describes the possible causes and solutions to vulnerability fix failures that occurred in the Security Center console.

Overview

Vulnerability fixes may fail due to various causes, such as an outdated system, incompatibility between the patch and the server, or a poor network connection. This topic covers the common causes of vulnerability fix failures. If the cause of a vulnerability fix failure is not mentioned in this topic, we recommend that you search the Internet for more information about the specific vulnerability to troubleshoot the failure.

Scenarios

You can reference this topic to troubleshoot fix failures for the following vulnerabilities:

- Linux software vulnerabilities
- Windows vulnerabilities
- Web-CMS vulnerabilities

Possible causes that lead to fix failures of Windows and Linux software vulnerabilities

If the system prompts that a fix failed when you fix a Windows or Linux software vulnerability in the Security Center console, see the following table to troubleshoot the failure.

> **Notice** We recommend that you identify the cause of a fix failure by following instructions in the table **from top to bottom**.

Possible cause	Description	Solution
The network connection is abnormal.	If a network connection error occurs on your server, the vulnerability fix may fail.	Troubleshoot the network connection error.
The Security Center agent of the server on which the vulnerability is detected is disconnected from Alibaba Cloud.	If the Security Center agent is disconnected from Alibaba Cloud, the vulnerability fix may fail. Network connection errors on the server, high CPU utilization, or high memory usage may cause the Security Center agent to disconnect from Alibaba Cloud.	Troubleshoot the Security Center agent disconnection. For more information, see Troubleshoot why the Security Center agent is offline.
The disk or memory space of the server on which the vulnerability is detected is insufficient.	If the disk does not have sufficient space, Security Center cannot download the patch package that is required to fix the vulnerability.	To troubleshoot this failure, perform the following steps: 1. Increase the storage space of the server or delete unnecessary files from the server. 2. Check whether the server can provide sufficient space. If yes, fix the vulnerability again in the Security Center console. For more information, see Linux software vulnerabilities and Windows vulnerabilities.

Possible cause	Description	Solution
No permissions are granted to read or write the disk file system of the server on which the vulnerability is detected.	If you do not have the read and write permissions on the disk file system, Security Center cannot download the patch package that is required to fix the vulnerability.	To troubleshoot this failure, perform the following steps: 1. Obtain the read and write permissions on the disk file system. 2. After you obtain the permissions, fix the vulnerability again in the Security Center console. For more information, see Linux software vulnerabilities and Windows vulnerabilities.
Linux vulnerability: Configuration errors occur in the system update source for the server on which the vulnerability is detected.	If configuration errors occur in the system update source or the YUM repositories are not up-to-date, Security Center cannot install the update as expected.	To troubleshoot this failure, perform the following steps: 1. Reconfigure the system update source. The following methods are available: ○ Log on to the and open the Vulnerabilities page. In the upper-right corner of the page, click **Settings**. In the panel that appears, select **Priority to use Alibaba Cloud source** for **YUM/APT Source Configuration**. After you select the option, Security Center automatically uses the YUM or APT source of Alibaba Cloud to download the update and fix the vulnerability. This increases the success rate of vulnerability fixes. ○ Make sure that the YUM repositories are up-to-date. 2. Fix the vulnerability again in the Security Center console. For more information, see Linux software vulnerabilities.
Linux vulnerability: The RPM database is corrupted.	If the RPM database is corrupted, Security Center cannot install the software package that is required to fix the vulnerability.	To troubleshoot this failure, perform the following steps: 1. Run the `rm -f /var/lib/rpm/_db.*` command to delete the RPM lock file. 2. Run the `rpm -rebuilddb` command to rebuild the RPM database. **Notice** This command may take a long time to run.

Possible cause	Description	Solution
Windows vulnerability: The prepatch for the vulnerability is missing.	If the prepatch for the vulnerability is missing, the vulnerability fix may fail.	To troubleshoot this failure, perform the following steps: 1. Install the prepatch. 2. After the prepatch is installed, fix the vulnerability again in the Security Center console. For more information, see Windows vulnerabilities.
Windows vulnerability: The Windows Update or Windows Modules Installer service is disabled on the server on which the vulnerability is detected.	If the Windows Update or Windows Modules Installer service is disabled, Security Center cannot download the patch package that is required to update the server system.	To troubleshoot this failure, perform the following steps: 1. Enable the Windows Update and Windows Modules Installer services. 2. Fix the vulnerability again in the Security Center console. For more information, see Windows vulnerabilities.
Windows vulnerability: Errors occurred during the downloading and installation of the patch package that is required to fix the vulnerability.	If the patch package is not found or is incompatible with the server operating system, the vulnerability fix may fail.	To troubleshoot this failure, perform the following steps: - The patch package is not found. Download the patch package again. Then, fix the vulnerability. - The patch package is incompatible with the server operating system. Log on to the Security Center console and ignore the vulnerability on the **Vulnerabilities** page. - Another patch is being installed. You cannot install two patches at the same time. We recommend that you fix the vulnerability after the current patch is installed.
Windows vulnerability: Other errors occur on the server.	None.	To troubleshoot this failure, perform the following steps: - Reset Windows Update components. For more information, see Windows Update - additional resources.

Possible causes that lead to fix failures of Web-CMS vulnerabilities

If the system prompts that a fix failed when you fix a Web-CMS vulnerability in the Security Center console, see the following table to troubleshoot the failure.

> **Note** We recommend that you identify the cause of a fix failure by following instructions in the table **from top to bottom**.

Possible cause	Description	Solution
The network connection is abnormal.	If a network connection error occurs on your server, the vulnerability fix may fail.	Troubleshoot the network connection error.
The Security Center agent of the server on which the vulnerability is detected is disconnected from Alibaba Cloud.	If the Security Center agent is disconnected from Alibaba Cloud, the vulnerability fix may fail. Network connection errors on the server, high CPU utilization, or high memory usage may cause the Security Center agent to disconnect from Alibaba Cloud.	Troubleshoot the Security Center agent disconnection. For more information, see Troubleshoot why the Security Center agent is offline.
The disk or memory space of the server on which the vulnerability is detected is insufficient.	If the disk does not have sufficient space, Security Center cannot download the patch package that is required to fix the vulnerability.	To troubleshoot this failure, perform the following steps: 1. Increase the storage space of the server or delete unnecessary files from the server. 2. Check whether the server can provide sufficient space. If yes, fix the vulnerability again in the Security Center console. For more information, see Web-CMS vulnerabilities.
Third-party security software is installed on the server on which the vulnerability is detected.	If security software, such as SafeDog, is installed on the server and you have optimized directory permissions or modified relevant settings by using the software, the system account may not have permissions to write the files in the `www` directory and its subdirectories. As a result, the vulnerability fix may fail.	Check whether the system account has the read and write permissions on the `www` directory and its subdirectories. If no, manually grant the permissions to the system account.
The vulnerability file does not exist.	If the vulnerability file is deleted, Security Center prompts that the fix failed.	To troubleshoot this failure, perform the following steps: 1. Check whether the vulnerability file is deleted from the specific server directory, which can be obtained from the vulnerability details in the Security Center console. 2. If the vulnerability file is deleted, ignore the vulnerability. For more information, see Ignore a vulnerability.

References

We recommend that you fix vulnerabilities at the earliest opportunity. Before you fix vulnerabilities, make sure that you understand the preparations and risk prevention measures. For more information, see Fix software vulnerabilities.

For more information about vulnerability fixes, see Vulnerability fixing.

2.Baseline check

2.1. Overview

The baseline check feature checks the configurations of server operating systems, databases, software, and containers. The feature also provides descriptions of check results and suggestions on security hardening. You can use the feature to harden the security of your assets, reduce the risks of intrusion, and meet the requirements for security compliance.

Baselines

Baselines describe the minimum requirements for security practices and compliance checks. The baseline check feature checks various configurations of operating systems, databases, and middleware, such as the configurations for weak passwords, account permissions, identity authentication, password policies, access control, security audit, and intrusion prevention. Security Center can check baseline configurations for threats to ensure security. The threats include weak passwords, unauthorized access, vulnerabilities, and configuration risks. Security Center can also check baseline configurations against the standards for classified protection compliance or the Center for Internet Security (CIS) standards to ensure compliance. You can use Security Center to check baseline configurations for more than 30 common versions of operating systems and for more than 10 types of databases and middleware. This way, you can help your enterprise meet various compliance requirements.

Description

The baseline check feature checks various configurations of operating systems and services, such as the configurations for weak passwords, account permissions, identity authentication, password policies, access control, security audit, and intrusion prevention. The feature also provides check results and suggestions on handling detected risks. The services include databases, software, and containers. For more information, see Baselines.

Security Center automatically checks all the assets within your Alibaba Cloud account from 00:00 to 06:00 every two days based on the default baseline check policy. You can create custom baseline check policies. You can also create custom weak password dictionaries and specify baseline check levels. The check levels are high, medium, and low. For more information, see Create baseline check policies.

Limits

The baseline check feature is a value-added feature of Security Center. Only users of the Advanced, Enterprise, and Ultimate editions can purchase and enable the feature. If you use the Basic or Anti-virus edition, you must upgrade Security Center to the Advanced, Enterprise, or Ultimate edition before you can use the baseline check feature. For more information about how to upgrade Security Center, see Upgrade and downgrade Security Center.

The following table describes the types of baselines that are supported by each edition.

Type	Basic edition	Anti-virus edition	Advanced edition	Enterprise edition	Ultimate edition
Weak password			√		
High risk exploit					

Type	Basic edition	Anti-virus edition	Advanced edition	Enterprise edition	Ultimate edition
Best security practice	×	×	×	√	√
Container security					
Classified protection compliance					
Custom baseline					

Note

- Users of Security Center Advanced can use only the default baseline check policy to run baseline checks. The users cannot create standard or custom baseline check policies.
- Users of the Enterprise and Ultimate editions of Security Center can use all baselines that are provided by the baseline check feature. The users can create standard and custom baseline check policies. The users can also edit and delete the baseline check policies that they create. The default baseline check policy cannot be deleted. If the Enterprise or Ultimate edition of Security Center detects baseline risks on Linux servers based on the Alibaba Cloud standards and the Multi-Level Protection Scheme (MLPS) standards, Security Center automatically fixes the risks.

Baselines

Category	Check standard and description	Involved operating system and service	Fixing description

Category	Check standard and description	Involved operating system and service	Fixing description
Weak password	Checks whether weak passwords are configured for your assets by using a method other than brute-force logons. The method does not lock your account, which prevents your workloads from being interrupted. **Note** Security Center detects weak passwords by comparing the hash value that is read by the system with the hash value that is calculated based on the weak password dictionary. If you do not want to enable the system to read the hash value, you can remove the baseline that detects weak passwords from your baseline check policy.	• Operating systems Linux and Windows • Databases MySQL, Redis, SQL Server, MongoDB, and PostgreSQL • Applications Tomcat, FTP, Rsync, and SVN	You must fix the baseline risks at the earliest opportunity. This way, you can prevent weak passwords from being exposed on the Internet. If weak passwords are exposed on the Internet, your assets can be attacked, and data breaches can occur.
High risk exploit	• Baselines that are used to check for unauthorized access Check whether unauthorized access risks exist in your services. This prevents intrusions and data breaches. • Baselines that are used to check for other high configuration risks Check whether high risks exist in the configurations of your services. This prevents vulnerabilities such as remote file read and remote command execution.	Memcached, Elasticsearch, Docker, CouchDB, ZooKeeper, Jenkins, Hadoop, and Tomcat	

Category	Check standard and description	Involved operating system and service	Fixing description
Best security practice	Alibaba Cloud standards Check whether risks exist in the configurations based on the Alibaba Cloud standards of best security practices. The configurations involve account permissions, identity authentication, password policies, access control, security audit, and intrusion prevention.	- Operating systems - CentOS 6, CentOS 7, and CentOS 8 - Red Hat 6 and Red Hat 7 - Ubuntu 12, Ubuntu 14, and Ubuntu 16 - Debian 8 - Alibaba Cloud Linux 2 - Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 - Databases MySQL, Redis, MongoDB, SQL Server, and Oracle Database 11g - Applications Tomcat, IIS, NGINX, and Apache	We recommend that you fix the detected risks. Security Center can reinforce the security of your assets based on the standards of best security practices. This prevents attacks and malicious modifications to the configurations of your assets.
Container security	Alibaba Cloud standards Check whether the Kubernetes master nodes contain risks based on the Alibaba Cloud standards of best practices for container security.	- Docker - Kubernetes cluster	

Category	Check standard and description	Involved operating system and service	Fixing description
Classified protection compliance	- The standards of MLPS level 2 and MLPS level 3 Check configurations based on the baselines for MLPS compliance for servers. The baseline checks meet the standards and requirements for computing environment that are proposed by authoritative assessment organizations. - CIS standards Check configurations based on the baselines for Center for Internet Security (CIS) compliance for operating systems.	- Operating systems involved in MLPS compliance ◦ CentOS 6, CentOS 7, and CentOS 8 ◦ Red Hat 6 and Red Hat 7 ◦ Ubuntu 12, Ubuntu 14, and Ubuntu 16 ◦ SUSE 10, SUSE 11, and SUSE 12 ◦ Debian 8 ◦ Alibaba Cloud Linux 2 ◦ Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 - Operating systems involved in CIS compliance ◦ CentOS 6 and CentOS 7 ◦ Ubuntu 12, Ubuntu 14, and Ubuntu 16 ◦ Debian 8 ◦ Alibaba Cloud Linux 2 ◦ Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019	We recommend that you fix the detected risks based on the compliance requirements for your business.
Custom baseline	Checks configurations based on custom baselines for CentOS Linux 7. You can specify or edit custom baselines in a custom baseline check policy based on your business requirements.	CentOS 7	We recommend that you fix the risks that are detected based on the custom baselines that you specify. Security Center can reinforce the security of your assets based on the standards of best security practices. This prevents attacks and malicious modifications to the configurations of your assets.

2.2. Baseline checks

Security Center provides default baseline checks. Security Center performs baseline checks on a server to detect risks and defects in the baseline configurations and applications of the server. If risks and defects are detected during baseline checks, Security Center generates alerts and provides fixing suggestions. This topic describes all baseline checks.

Category	Baseline check	Description	Number of check items
	Zabbix login weak password baseline	Checks weak passwords that are used to log on to Zabbix.	1
	Samba login weak password detection	Checks weak passwords for users of Samba databases.	1
	ElasticSearch login weak password baseline	Checks weak passwords that are used to log on to Elasticsearch servers.	1
	Activemq login weak password baseline	Checks weak passwords that are used to log on to ActiveMQ.	1
	RabbitMQ login weak password baseline	Checks weak passwords that are used to log on to RabbitMQ.	1
	OpenVPN weak password detection in Linux system	Checks common weak passwords of OpenVPN accounts in Linux operating systems.	1
	Jboss6/7 login weak password baseline	Checks weak passwords that are used to log on to JBoss 6 and JBoss 7.	1
	Jenkins login weak password baseline	Checks weak passwords that are used to log on to Jenkins. This baseline check provides more samples to detect weak passwords than its earlier version.	1
	Proftpd login weak password baseline	Checks weak passwords that are used to log on to ProFTPD. This baseline check provides more samples to detect weak passwords than its earlier version.	1
	Influxdb login weak password baseline	Checks weak passwords that are used to log on to InfluxDB databases. This baseline check provides more samples to detect weak passwords than its earlier version.	1
	Weblogic 12c login weak password detection	Checks weak password for users of WebLogic Server 12c.	1
	Openldap login weak password baseline	Checks weak passwords that are used to log on to OpenLDAP.	1

Category	Baseline check	Description	Number of check items
Weak password	VncServer weak password check	Checks common weak passwords that are used to log on to the VNC service.	1
	pptpd login weak password baseline	Checks weak passwords that are used to log on to PPTP servers.	1
	Oracle login weak password detection	Checks weak passwords for users of Oracle databases.	1
	svn login weak password baseline	Checks weak passwords that are used to log on to Subversion (SVN) servers.	1
	rsync login weak password baseline	Checks weak passwords that are used to log on to rsync servers.	1
	MongoDB Weak Password baseline	Checks weak passwords for the MongoDB service. MongoDB 3.x and 4.x support this baseline check.	1
	PostgreSQL DB login weak password baseline	Checks weak passwords that are used to log on to PostgreSQL databases.	1
	SQL Server DB login weak password baseline	Checks weak passwords that are used to log on to Microsoft SQL Server databases.	1
	Mysql DB login weak password baseline(Windows version)	Checks weak passwords that are used to log on to MySQL databases. This baseline check is suitable only for Windows operating systems.	1
	Apache Tomcat Console weak password baseline	Checks weak passwords that are used to log on to the Apache Tomcat console. Apache Tomcat 7, 8, and 9 support this baseline check.	1
	Ftp login weak password baseline	Checks weak passwords that are used to log on to FTP servers and anonymous logons to FTP servers.	1
	Redis DB login weak password baseline	Checks weak passwords that are used to log on to Redis databases.	1
	Windows system login weak password baseline	Checks weak passwords that are used to log on to Windows Server operating systems. This baseline check provides more samples to detect weak passwords than its earlier version.	1
	Linux system login weak password baseline	Checks weak passwords that are used to log on to Linux operating systems. This baseline check provides more samples to detect weak passwords than its earlier version.	1

Category	Baseline check	Description	Number of check items
	Mysql DB login weak password baseline	Checks weak passwords that are used to log on to MySQL databases. This baseline check provides more samples to detect weak passwords than its earlier version.	1
	MongoDB Weak Password baseline(support version 2. X)	Checks weak passwords for users of the MongoDB service.	1
Unauthorized access	Influxdb unauthorized access high exploit vulnerability risk	Checks InfluxDB vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Redis unauthorized access high exploit vulnerability risk	Checks Redis vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Jboss unauthorized access high exploit vulnerability risk	Checks JBoss vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	ActiveMQ unauthorized access high exploit vulnerability risk	Checks ActiveMQ vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	RabbitMQ unauthorized access high exploit vulnerability risk	Checks RabbitMQ vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	OpenLDAP unauthorized access vulnerability baseline (Linux)	Checks OpenLDAP vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Kubernetes-Apiserver unauthorized access to high-risk risks	Checks Kubernetes API server vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	LDAP unauthorized access high exploit vulnerability risk (Windows)	Checks LDAP vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	rsync unauthorized access high exploit vulnerability risk	Checks rsync vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Mongodb unauthorized access high exploit vulnerability risk	Checks MongoDB vulnerabilities that can be exploited by attackers to implement unauthorized access.	1

Category	Baseline check	Description	Number of check items
	Postgresql unauthorized access to high-risk risk baseline	Checks PostgreSQL vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Jenkins unauthorized access high exploit vulnerability risk	Checks Jenkins vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Hadoop unauthorized access high exploit vulnerability risk	Checks Apache Hadoop vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	CouchDB unauthorized access high exploit risk	Checks Apache CouchDB vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	ZooKeeper unauthorized access high exploit vulnerability risk	Checks Apache ZooKeeper vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Docker unauthorized access high vulnerability risk	Checks Docker vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Memcached unauthorized access high exploit vulnerability risk	Checks memcached vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
	Elasticsearch unauthorized access high exploit vulnerability risk	Checks Elasticsearch vulnerabilities that can be exploited by attackers to implement unauthorized access.	1
Container	CIS standard-Kubernetes(ACK) node security inspection inspection	Checks the baseline against the Center for Internet Security (CIS) standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	52
	CIS standard-Kubernetes(ACK) Master node security inspection inspection	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	8

Container security Category	Baseline check	Description	Number of check items
	Alibaba Cloud Standard-Kubernetes-Node security baseline check	Checks the baseline against the Alibaba Cloud standard of best practices for Kubernetes Master.	7
	Alibaba Cloud Standard-Kubernetes-Master security baseline check	Checks the baseline against the Alibaba Cloud standard of best practices for Kubernetes Master.	18
	Alibaba Cloud Standard -DockerSecurity Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Docker.	17
	Alibaba Cloud Linux/Aliyun Linux 2 Benchmark	Checks the baseline against the Alibaba Cloud standard of best practices for Alibaba Cloud Linux 2.	15
	Alibaba Cloud Standard - CentOS Linux 6 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for CentOS Linux 6.	15
	Alibaba Cloud Standard - CentOS Linux 7/8 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for CentOS Linux 7 and CentOS Linux 8.	15
	Alibaba Cloud Standard - Debian Linux 8/9/10 Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for Debian Linux 8, Debian Linux 9, and Debian Linux 10.	15
	Alibaba Cloud Standard - Red Hat Enterprise Linux 6 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Red Hat Enterprise Linux (RHEL) 6.	15
	Alibaba Cloud Standard - Red Hat Enterprise Linux 7/8 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for RHEL 7 and RHEL 8.	15
	Alibaba Cloud Standard - Ubuntu Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for Ubuntu.	15
	Alibaba Cloud Standard - Windows Server 2008 R2 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Windows Server 2008 R2.	12

Category	Baseline check	Description	Number of check items
Best security practice	Alibaba Cloud Standard - Windows 2012 R2 Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for Windows Server 2012 R2.	12
	Alibaba Cloud Standard - Windows 2016/2019 Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for Windows Server 2016 and Windows Server 2019.	12
	Alibaba Cloud Standard-SQL Server Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for SQL Server 2012.	17
	Alibaba Cloud Standard - Memcached Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for memcached.	5
	Alibaba Cloud Standard - MongoDB version 3.x Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for MongoDB.	9
	Alibaba Cloud Standard - Mysql Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for MySQL. MySQL 5.1 to MySQL 5.7 support this baseline check.	12
	Alibaba Cloud Standard - Oracle 11g Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Oracle Database 11g.	14
	Alibaba Cloud Standard-PostgreSql Security Initialization Check	Checks the baseline against the Alibaba Cloud standard of best practices for PostgreSQL.	11
	Alibaba Cloud Standard - Redis Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Redis.	7
	Alibaba Cloud Standard - Anolis 8 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Anolis 8.	15
	Alibaba Cloud Standard - Apache Security Baseline Check	Checks the baseline of middleware against the standards of CIS and Alibaba Cloud.	19
	Alibaba cloud standard - CouchDB security baseline check	Checks the baseline against the Alibaba Cloud standard for Apache CouchDB.	5

Category	Baseline check	Description	Number of check items
	Alibaba Cloud Standard - ElasticSearch Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Elasticsearch.	3
	Alibaba Cloud Standard - Hadoop Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Apache Hadoop.	3
	Alibaba Cloud Standard - IIS 8 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Internet Information Services (IIS) 8.	8
	Alibaba Cloud Standard - Influxdb Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for InfluxDB.	5
	Alibaba Cloud Standard -Jboss6/7 Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for JBoss 6 and JBoss 7.	11
	Alibaba Cloud Standard - Kibana Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Kibana.	4
	Alibaba Cloud Standard - Kylin Security Baseline Check	Checks the baseline against the Alibaba Cloud standard for Kylin.	15
	Alibaba Cloud Standard -Activemq Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for ActiveMQ.	7
	Alibaba Cloud Standard - Jenkins Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Jenkins.	6
	Alibaba Cloud Standard - RabbitMQ Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for RabbitMQ.	4
	Alibaba Cloud Standard - Nginx Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for NGINX.	13
	Alibaba Cloud Standard - Windows SMB Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for Windows SMB.	2
	Alibaba Cloud Standard - SUSE Linux 15 Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for SUSE Linux 15.	15

Category	Baseline check	Description	Number of check items
	Alibaba Cloud Standard - Apache Tomcat Security Baseline(on windows)	Checks the baseline of middleware against the standards of CIS and Alibaba Cloud.	8
	Alibaba Cloud Standard - Uos Security Baseline Check	Checks the baseline against the Alibaba Cloud standard of best practices for UOS.	15
	Alibaba Cloud Standard - Zabbix Security Baseline	Checks the baseline against the Alibaba Cloud standard of best practices for Zabbix.	6
	Alibaba Cloud Standard-Apache Tomcat Security Baseline	Checks the baseline of middleware against the standards of CIS and Alibaba Cloud.	13
	Alibaba Cloud Linux/Aliyun Linux 2 CIS Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	178
	CIS CentOS Linux 6 LTS Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	196
	CIS CentOS Linux 7 LTS Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	197
	CIS CentOS Linux 8 LTS Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	164

Category	Baseline check	Description	Number of check items
CIS compliance	CIS Debian Linux 8 Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	155
	CIS Ubuntu Linux 14 LTS Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	177
	CIS Ubuntu Linux 16/18/20 LTS Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	176
	CIS Microsoft Windows Server 2008 R2 Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	274
	CIS Microsoft Windows Server 2012 R2 Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	275
	CIS Microsoft Windows Server 2016/2019 R2 Benchmark	Checks the baseline against the CIS standard. This standard is suitable for enterprise users who have professional security skills. This baseline check provides a variety of check rules, which allows you to reinforce the security of your system based on business scenarios and requirements.	275
	SUSE Linux 15 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for SUSE Linux Enterprise Server 15. This checks whether your asset environments comply with the classified protection requirements.	18
	Alibaba Cloud Linux 3 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Alibaba Cloud Linux 3. This checks whether your asset environments comply with the classified protection requirements.	19

Category	Baseline check	Description	Number of check items
	Alibaba Cloud Linux/Aliyun Linux 2 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Alibaba Cloud Linux 2. This checks whether your asset environments comply with the classified protection requirements.	19
	China's Level 3 Protection of Cybersecurity - Bind Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Bind. This checks whether your asset environments comply with the classified protection requirements.	4
	CentOS Linux 6 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for CentOS Linux 6. This checks whether your asset environments comply with the classified protection requirements.	19
	CentOS Linux 7 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for CentOS Linux 7. This checks whether your asset environments comply with the classified protection requirements.	19
	CentOS Linux 8 Baseline for China classified protection of cybersecurity - Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for CentOS Linux 8. This checks whether your asset environments comply with the classified protection requirements.	19
	IIS Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Oracle. This checks whether your asset environments comply with the classified protection requirements.	5
	China's Level 3 Protection of Cybersecurity - Informix Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Informix. This checks whether your asset environments comply with the classified protection requirements.	6
	China's Level 3 Protection of Cybersecurity - Jboss6/7 Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for JBoss 6 or JBoss 7. This checks whether your asset environments comply with the classified protection requirements.	5
	MongoDB Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for MongoDB. This checks whether your asset environments comply with the classified protection requirements.	6

Category	Baseline check	Description	Number of check items
	China's Level 3 Protection of Cybersecurity -SQL Server Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for SQL Server. This checks whether your asset environments comply with the classified protection requirements.	4
	Equal Guarantee Level 3-MySql Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for MySQL. This checks whether your asset environments comply with the classified protection requirements.	5
	Equal Guarantee Level 3-Nginx Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for NGINX. This checks whether your asset environments comply with the classified protection requirements.	3
	China's Level 3 Protection of Cybersecurity - Oracle Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Oracle. This checks whether your asset environments comply with the classified protection requirements.	12
	Level 3-PostgreSql compliance baseline check	Checks the baseline against the standard of MLPS 2.0 level 3 for PostgreSQL. This checks whether your asset environments comply with the classified protection requirements.	4
	China's Level 3 Protection of Cybersecurity - Red Hat Enterprise Linux 6 Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Red Hat Enterprise Linux 6. This checks whether your asset environments comply with the classified protection requirements.	19
	China's Level 3 Protection of Cybersecurity - Red Hat Enterprise Linux 7 Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Red Hat Enterprise Linux 7. This checks whether your asset environments comply with the classified protection requirements.	19
	Redis Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Redis. This checks whether your asset environments comply with the classified protection requirements.	4
	SUSE Linux 10 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for SUSE Linux Enterprise Server 10. This checks whether your asset environments comply with the classified protection requirements.	19

Category	Baseline check	Description	Number of check items
Operating systems involved in MLPS compliance	SUSE Linux 12 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for SUSE Linux Enterprise Server 12. This checks whether your asset environments comply with the classified protection requirements.	19
	SUSE Linux 11 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for SUSE Linux Enterprise Server 11. This checks whether your asset environments comply with the classified protection requirements.	19
	Ubuntu 14 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Ubuntu 14. This checks whether your asset environments comply with the classified protection requirements.	19
	Waiting for Level 3-Ubuntu 16/18/20 compliance regulations inspection	Checks the baseline against the standard of MLPS 2.0 level 3 for Ubuntu 16, Ubuntu 18, and Ubuntu 20. This checks whether your asset environments comply with the classified protection requirements.	19
	China's Level 3 Protection of Cybersecurity - Websphere Application Server Compliance Baseline Check	Checks the baseline against the standard of Multi-Level Protection Scheme (MLPS) 2.0 level 3 for WebSphere Application Server. This checks whether your asset environments comply with the classified protection requirements.	7
	Weblogic Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Oracle WebLogic Server. This checks whether your asset environments comply with the classified protection requirements.	5
	China's Level 3 Protection of Cybersecurity - Windows Server 2008 R2 Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Windows Server 2008 R2. This checks whether your asset environments comply with the classified protection requirements.	19
	Windows 2012 R2 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Windows Server 2012 R2. This checks whether your asset environments comply with the classified protection requirements.	19
	Windows 2016/2019 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Windows Server 2016 R2 and 2019 R2. This checks whether your asset environments comply with the classified protection requirements.	19

Category	Baseline check	Description	Number of check items
	Alibaba Cloud Linux/Aliyun Linux 2 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Alibaba Cloud Linux 2. This checks whether your asset environments comply with the classified protection requirements.	15
	CentOS Linux 6 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for CentOS Linux 6. This checks whether your asset environments comply with the classified protection requirements.	15
	CentOS Linux 7 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for CentOS Linux 7. This checks whether your asset environments comply with the classified protection requirements.	15
	Debian Linux 8 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Debian Linux 8. This checks whether your asset environments comply with the classified protection requirements.	12
	Redhat Linux 7 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Red Hat Enterprise Linux 7. This checks whether your asset environments comply with the classified protection requirements.	15
	Linux Ubuntu 16/18 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Ubuntu 16 and Ubuntu 18. This checks whether your asset environments comply with the classified protection requirements.	19
	Windows 2008 R2 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Windows Server 2008 R2. This checks whether your asset environments comply with the classified protection requirements.	12
	Windows 2012 R2 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Windows Server 2012 R2. This checks whether your asset environments comply with the classified protection requirements.	12
	Windows 2016/2019 Baseline for China classified protection of cybersecurity-Level II	Checks the baseline against the standard of MLPS 2.0 level 2 for Windows Server 2016 R2 and 2019 R2. This checks whether your asset environments comply with the classified protection requirements.	12
	Debian Linux 8/9/10 Baseline for China classified protection of cybersecurity-Level III	Checks the baseline against the standard of MLPS 2.0 level 3 for Debian Linux 8, Debian Linux 9, and Debian Linux 10. This checks whether your asset environments comply with the classified protection requirements.	19

Category	Baseline check	Description	Number of check items
	China's Level 3 Protection of Cybersecurity - Kylin Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Kylin. This checks whether your asset environments comply with the classified protection requirements.	19
	China's Level 3 Protection of Cybersecurity - uos Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for UOS. This checks whether your asset environments comply with the classified protection requirements.	19
	China's Level 3 Protection of Cybersecurity - Anolis 8 Compliance Baseline Check	Checks the baseline against the standard of MLPS 2.0 level 3 for Anolis 8. This checks whether your asset environments comply with the classified protection requirements.	19
Custom baseline	Alibaba cloud standard Ubuntu custom security baseline check	Checks the custom baseline against the Alibaba Cloud standard of best practices for Ubuntu 14, Ubuntu 16, Ubuntu 18, and Ubuntu 20.	62
	Windows custom baseline	The custom template that contains all baseline check items related to Windows. You can select baseline check items and configure parameters for baseline check items by using the template. This helps best suit your business requirements.	63
	CentOS Linux 6 custom baseline	The custom template that contains all baseline check items related to CentOS Linux 6. You can select baseline check items and configure parameters for baseline check items by using the template. This helps best suit your business requirements.	47
	CentOS Linux 7/8 custom baseline	The custom template that contains all baseline check items related to CentOS Linux 7 and CentOS Linux 8. You can select baseline check items and configure parameters for baseline check items by using the template. This helps best suit your business requirements.	53

2.3. Create baseline check policies

Security Center allows you to create baseline check policies. You can run baseline checks on your assets to detect baseline risks based on baseline check policies. This topic describes how to create baseline check policies.

Prerequisites

Context

Security Center checks all the assets within your Alibaba Cloud account from 00:00 to 06:00 every two days based on the **default baseline check policy**. You can click **Edit** in the Actions column in the right area of **Default** in the Manage Policies panel of the Baseline Check page to go to the **Check Policy** panel. In the Check Policy panel, you can view the baselines that are included in the **default baseline check policy** in the **Check Items** section. Weak password

If the **default baseline check policy** cannot meet your requirements for baseline checks, you can click **Add standard policy** and **Add custom policy** to create standard and custom baseline check policies. In this case, you can specify the baselines that are not included in the **default baseline check policy**.

Note Only users of the Enterprise and Ultimate editions can create **standard** and **custom** baseline check policies. Users of Security Center Advanced can run baseline checks only based on the **default baseline check policy**.

The following table describes the baseline types, number of baselines, Security Center editions, and use scenarios that are supported by different types of baseline check policies. The policies are default baseline check, standard baseline check, and custom baseline check policies.

Policy	Security Center edition	Baseline type	Number of baselines	Modification	Use scenario
Default baseline check policy	Advanced, Enterprise, and Ultimate	• High risk exploit • Container security • Best security practices • Weak password	Greater than or equal to 70	Not supported.	The default baseline check policy provided by Security Center is used to check whether risks exist in the configurations of your assets based on the following types of baselines: high risk exploit, container security, best security practice, and weak password.

Policy	Security Center edition	Baseline type	Number of baselines	Modification	Use scenario
Standard baseline check policy	Enterprise and Ultimate	- High risk exploit - Container security - Classified protection compliance - Best security practices - Weak password	Greater than or equal to 120	You can modify policy parameters.	Compared with the default baseline check policy, standard baseline check policies support one more baseline type: classified protection compliance. For the baseline types that are supported by the two types of policies, standard baseline check policies support more baselines. In addition, you can modify policy parameters. You can create standard baseline check policies based on your business requirements. For more information, see Create a standard baseline check policy.
Custom baseline check policy	Enterprise and Ultimate	Custom baselines for operating systems	Greater than or equal to 50	You can modify policy parameters. You can also modify the parameters of some baselines.	Custom baseline check policies are used to check whether risks exist in the configurations of your assets based on the custom baselines for operating systems. You can create custom baseline check policies and modify the parameters of baselines based on your business requirements. For more information, see Create a custom baseline check policy.

Security Center provides default rules to detect weak passwords based on Alibaba Cloud threat intelligence. You can also create custom rules to detect weak passwords based on your business requirements. For more information, see Create custom rules to detect weak passwords.

Create a standard baseline check policy

Compared with the default baseline check policy, standard baseline check policies support one more baseline type: classified protection compliance. For the baseline types that are supported by the two types of policies, standard baseline check policies support more baselines. In addition, you can modify policy parameters. You can create a standard baseline check policy to check baseline configurations of your assets in a more comprehensive manner.

1.
2.
3.

4. In the **Manage Policies** panel, click **Add standard policy**.
5. In the **Check Policy** panel, configure the parameters.

   The following table describes the parameters.

Parameter	Description
Policy Name	The name of the policy.
Schedule	The interval at which baseline checks are performed. Valid values: 1 day, 3 Day(s), 7 Day(s), and 30 Day(s).
Detection time	The time range during which baseline checks are performed. Valid values: 00:00 - 06:00, 06:00 - 12:00, 12:00 - 18:00, and 18:00 - 24:00.
Check Items	The baselines that you want to use. For more information, see Baselines.
Servers	The server groups on which you want to run baseline checks based on the policy. ? **Note** By default, newly purchased servers belong to **All Groups > Default**.To apply the policy to newly purchased servers, you must select **Default**. For more information about how to add or modify a server group, see Manage asset groups.

6. Click **Ok**. The standard baseline check policy is created.

   Security Center runs baseline checks on your assets based on the policy that you create.

Create custom rules to detect weak passwords

You can create custom rules based on the default rules that are provided by Security Center to detect weak passwords. You can use custom rules to better meet your business requirements and detect weak passwords in a more comprehensive manner.

1.
2.
3.
4. In the **Custom Weak Password Rules** section, create custom rules to detect weak passwords.

   You can use one of the following methods to create custom rules:

   - Upload rules by using the weak password template.
     a. Click **Download** next to Template.
     b. Configure rules in the downloaded template based on your business requirements and save the template.

   c. Click **Import File** to upload the template. Custom rules to detect weak passwords are created.
      Security Center checks whether weak passwords are configured for your assets based on the custom rules.

      > ⓘ **Note** Before you upload the template, make sure that the following requirements are met:
      >
      > - The size of the file does not exceed 5 KB.
      > - Each line in the file contains only one weak password. Otherwise, Security Center cannot accurately detect weak passwords.
      > - The file contains up to 2,000 weak passwords.

- Create a custom dictionary of weak passwords.

   a. Click **Custom weak password dictionary** next to Weak password.

   b. In the **Custom weak password dictionary** panel, configure the parameters.

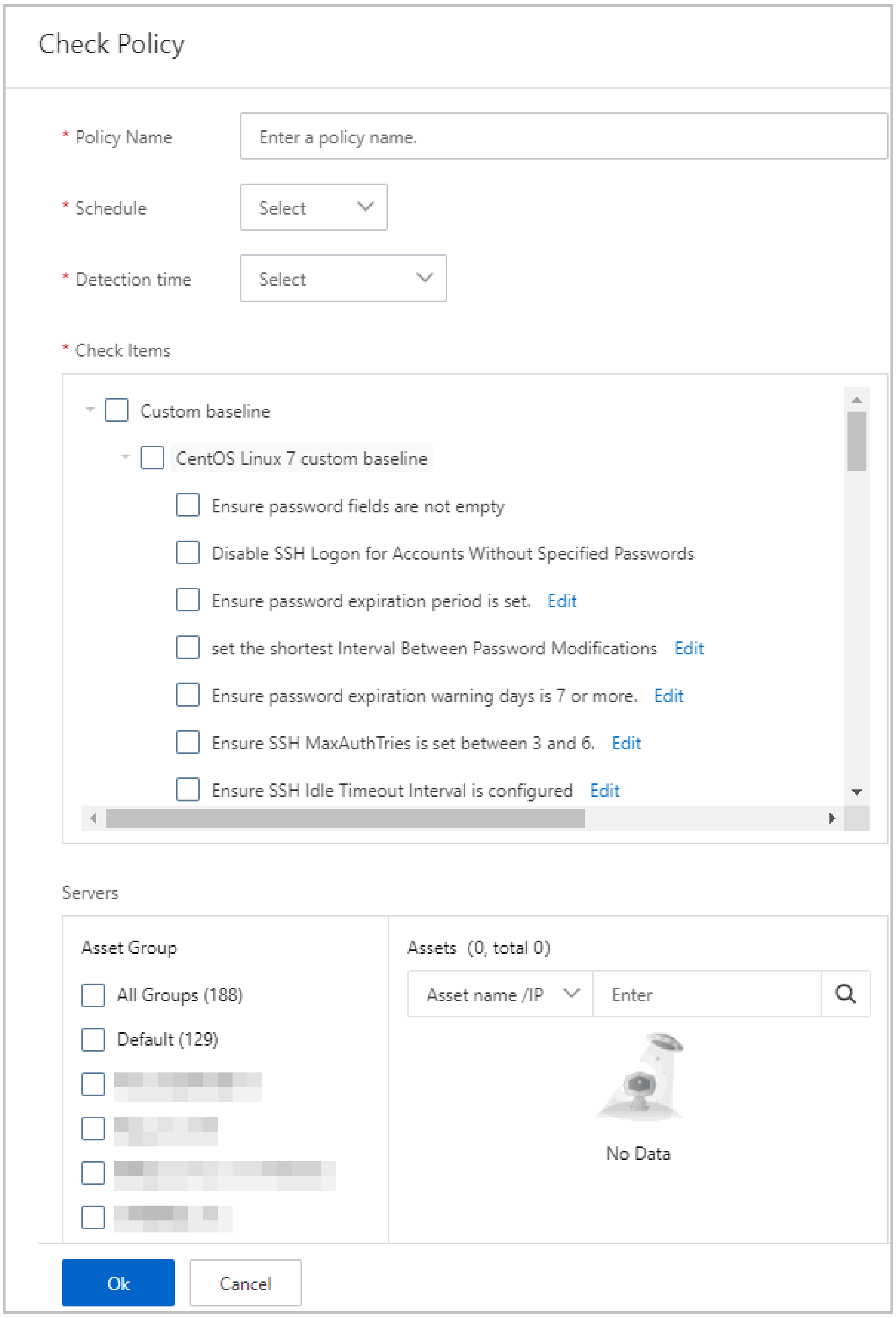
Parameter	Description
Domain	The domain name of your asset.
Company name	The name of your enterprise.
Keyword	The passwords that you want to add to the dictionary.
Weak password dictionary	You do not need to configure this parameter. This weak password dictionary is provided by Security Center based on Alibaba Cloud threat intelligence.

   c. Click **Generate and Import**. The custom dictionary of weak passwords is created.
      Security Center checks whether weak passwords are configured for your assets based on the created custom dictionary of weak passwords.

Create a custom baseline check policy

You can create a custom baseline check policy to check whether risks exist in the configurations of your assets based on the custom baselines for operating systems.

1.
2.
3.
4. In the **Manage Policies** panel, click **Add custom policy**.
5. In the **Check Policy** panel, configure the parameters.



Check Policy

* Policy Name: Enter a policy name.

* Schedule: Select

* Detection time: Select

* Check Items

- □ Custom baseline
  - □ CentOS Linux 7 custom baseline
    - □ Ensure password fields are not empty
    - □ Disable SSH Logon for Accounts Without Specified Passwords
    - □ Ensure password expiration period is set. Edit
    - □ set the shortest Interval Between Password Modifications Edit
    - □ Ensure password expiration warning days is 7 or more. Edit
    - □ Ensure SSH MaxAuthTries is set between 3 and 6. Edit
    - □ Ensure SSH Idle Timeout Interval is configured Edit

Servers

Asset Group

- □ All Groups (188)
- □ Default (129)
- □
- □
- □
- □

Assets (0, total 0)

Asset name /IP | Enter

No Data

Ok | Cancel

The following table describes the parameters.

Parameter	Description
Policy Name	The name of the policy.
Schedule	The interval at which baseline checks are performed. Valid values: 1 day, 3 Day(s), 7 Day(s), and 30 Day(s).
Detection time	The time range during which baseline checks are performed. Valid values: 00:00 - 06:00, 06:00 - 12:00, 12:00 - 18:00, and 18:00 - 24:00.

Parameter	Description
Check Items	The baselines that you want to use. For more information, see Baselines. ⓘ **Note** You can modify the parameters of some custom baselines based on your business requirements.
Servers	The server groups on which you want to run baseline checks based on the policy. ⓘ **Note** ○ You can apply only one custom baseline check policy to the servers that belong to the same server group. If a server group is selected for a custom baseline check policy, you can no longer select the server group for the Servers parameter when you create a custom baseline check policy. ○ By default, newly purchased servers belong to **All Groups > Default**. To apply the policy to newly purchased servers, you must select **Default**. For more information about how to add or modify a server group, see Manage asset groups.

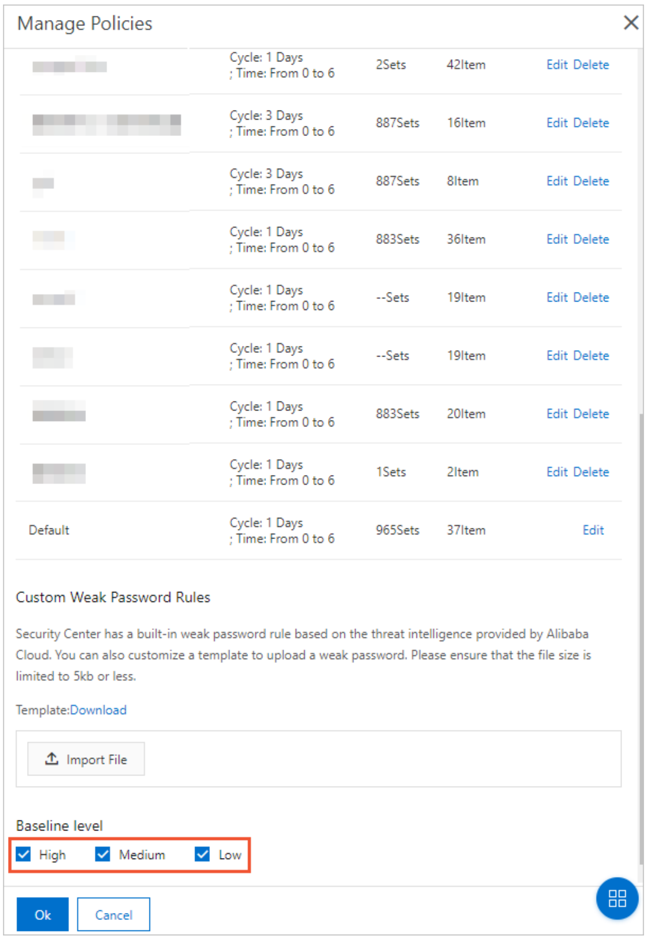
6. Click **Ok**. The custom baseline check policy is created.

   Security Center runs baseline checks on your assets based on the policy that you create.

Manage a baseline check policy

After you create a baseline check policy, you can configure **Baseline level** based on your business requirements. You can also click **Edit** or **Delete** to modify or delete a baseline check policy.

- In the lower part of the **Manage Policies** panel, you can configure Baseline level. Valid values: **High**, **Medium**, and **Low**.



Manage Policies

[redacted]	Cycle: 1 Days ; Time: From 0 to 6	2Sets	42Item	Edit Delete
[redacted]	Cycle: 3 Days ; Time: From 0 to 6	887Sets	16Item	Edit Delete
[redacted]	Cycle: 3 Days ; Time: From 0 to 6	887Sets	8Item	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	883Sets	36Item	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	--Sets	19Item	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	--Sets	19Item	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	883Sets	20Item	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	1Sets	2Item	Edit Delete
Default	Cycle: 1 Days ; Time: From 0 to 6	965Sets	37Item	Edit

Custom Weak Password Rules

Security Center has a built-in weak password rule based on the threat intelligence provided by Alibaba Cloud. You can also customize a template to upload a weak password. Please ensure that the file size is limited to 5kb or less.

Template:Download

Baseline level

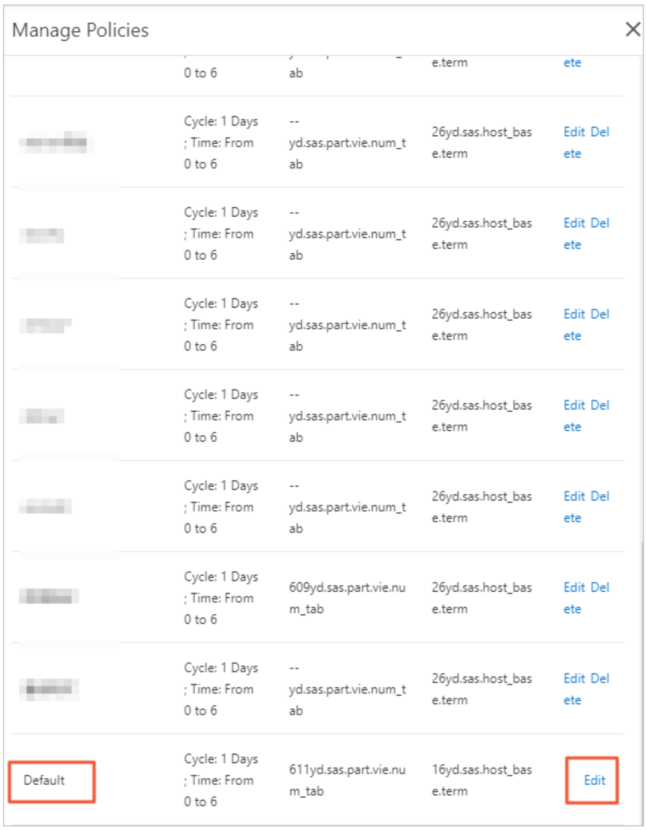
☑ High ☑ Medium ☑ Low

- In the Manage Policies panel, you can click **Edit** or **Delete** in the **Actions** column for a policy to modify or delete the policy.

> **Note** You cannot restore a policy after you delete it.

- In the Manage Policies panel, you can find the **default baseline check** policy and click **Edit** in the **Actions** column to modify the server groups to which the policy is applied.

> **Note** You cannot delete the default baseline check policy or modify the baselines of the default baseline check policy. You can only modify the server groups to which the default baseline check policy is applied.


Manage Policies

	0 to 6	ab	e.term	ete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	-- yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	-- yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	-- yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	-- yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	-- yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	609yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
[redacted]	Cycle: 1 Days ; Time: From 0 to 6	-- yd.sas.part.vie.num_tab	26yd.sas.host_base.term	Edit Delete
Default	Cycle: 1 Days ; Time: From 0 to 6	611yd.sas.part.vie.num_tab	16yd.sas.host_base.term	Edit

Operations

After you create a baseline check policy, you can use Security Center to check whether risks exist in your assets based on the baseline check policy. For more information, see Run a baseline check.

2.4. Run a baseline check

The Advanced and Enterprise editions of Security Center provide the baseline check feature to detect baseline risks on your servers. This topic describes how to run a baseline check.

Prerequisites

-
- A custom policy for baseline checks is created. For more information, see Create baseline check policies.

> ? **Note** Only the Enterprise edition of Security Center supports custom policies for baseline checks. If no custom policies are created, Security Center runs baseline checks based on the default policy. The default policy does not cover all check items. Therefore, the items that you want to check may not be included in the policy.

Context

For more information about check items, see Baselines.

The baseline check feature supports manual checks and periodic checks that run automatically.

- **Periodic and automatic checks:** periodic checks that run automatically based on the default policy or custom policies. The default policy automatically starts a baseline check at 00:00:00 every second day.

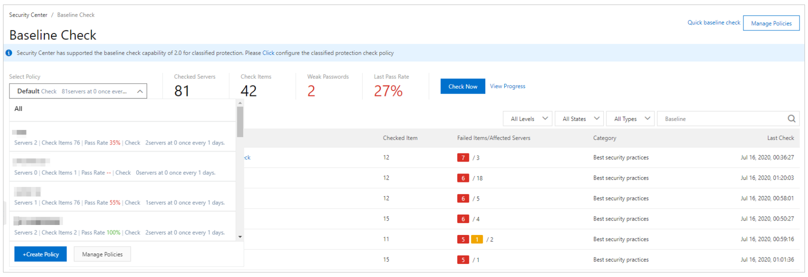
- **Manual checks**: If you have created or modified a custom policy, you can select it in the **Select Policy** drop-down list on the **Baseline Check** page, and click Check Now to start a manual check. Manual baseline checks allow you to scan for baseline risks in real time.

Run a manual baseline check

1.

2.

3. In the **Select Policy** drop-down list, select a policy to run a manual check.



Security Center / Baseline Check

Baseline Check

Quick baseline check | Manage Policies

Security Center has supported the baseline check capability of 2.0 for classified protection. Please Click configure the classified protection check policy

Select Policy: Default Check 81servers at 0 once ever...

Checked Servers 81 | Check Items 42 | Weak Passwords 2 | Last Pass Rate 27%

Check Now | View Progress

All

[redacted]
Servers 2 | Check Items 76 | Pass Rate 35% | Check 2servers at 0 once every 1 days.

[redacted]
Servers 0 | Check Items 1 | Pass Rate -- | Check 0servers at 0 once every 1 days.

[redacted]
Servers 1 | Check Items 76 | Pass Rate 55% | Check 1servers at 0 once every 1 days.

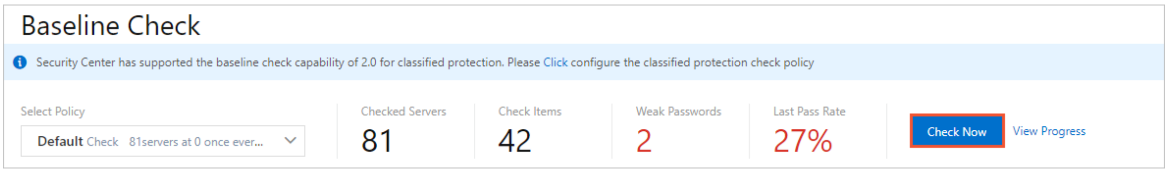
[redacted]
Servers 2 | Check Items 2 | Pass Rate 100% | Check 2servers at 0 once every 1 days.

+Create Policy | Manage Policies

All Levels | All States | All Types | Baseline

Checked Item	Failed Items/Affected Servers	Category	Last Check
12	7 / 3	Best security practices	Jul 16, 2020, 00:36:27
12	6 / 18	Best security practices	Jul 16, 2020, 01:20:03
12	6 / 5	Best security practices	Jul 16, 2020, 00:58:01
15	6 / 4	Best security practices	Jul 16, 2020, 00:50:27
11	5 1 / 2	Best security practices	Jul 16, 2020, 00:59:16
15	5 / 1	Best security practices	Jul 16, 2020, 01:01:36

4. Click **Check Now**.



Baseline Check

Security Center has supported the baseline check capability of 2.0 for classified protection. Please Click configure the classified protection check policy

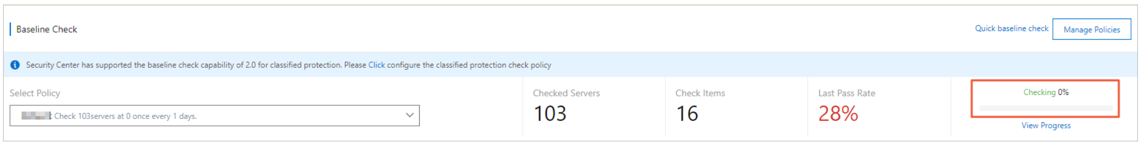
Select Policy: Default Check 81servers at 0 once ever...

Checked Servers 81 | Check Items 42 | Weak Passwords 2 | Last Pass Rate 27%

Check Now | View Progress

You can view the task progress and detailed check results.

- The progress is updated in the View Progress section in real time.



Baseline Check

Quick baseline check | Manage Policies

Security Center has supported the baseline check capability of 2.0 for classified protection. Please Click configure the classified protection check policy

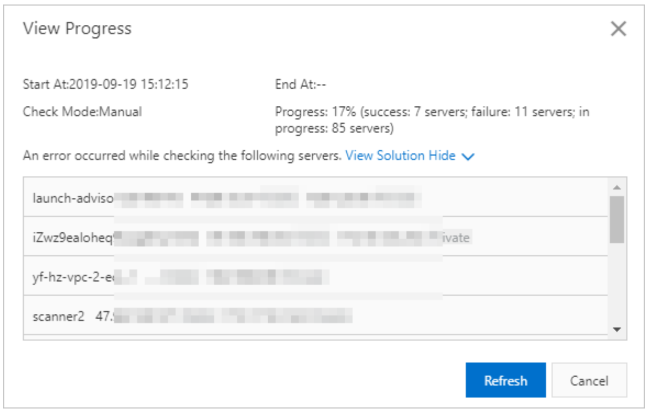
Select Policy: [redacted] Check 103servers at 0 once every 1 days.

Checked Servers 103 | Check Items 16 | Last Pass Rate 28%

Checking 0%

View Progress

- You can click **View Progress** to view the task details, including the number of servers that complete the check, number of servers that fail the check, and causes of check failures. You can click **View Solution** to view the solutions on how to handle failures.



View Progress

Start At:2019-09-19 15:12:15

End At:--

Check Mode:Manual

Progress: 17% (success: 7 servers; failure: 11 servers; in progress: 85 servers)

An error occurred while checking the following servers. View Solution Hide

launch-adviso[redacted]

iZwz9ealoheq[redacted]ivate

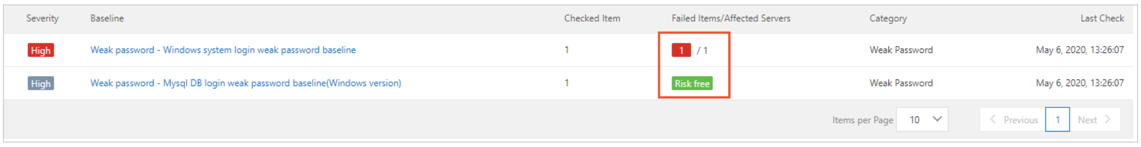
yf-hz-vpc-2-e[redacted]

scanner2 47.[redacted]

Refresh | Cancel

You can click **Refresh** to update the progress.

- View baseline risks in the result list.
After the baseline check is completed, the result is displayed on the **Baseline Check** page.



Severity	Baseline	Checked Item	Failed Items/Affected Servers	Category	Last Check
High	Weak password - Windows system login weak password baseline	1	1 / 1	Weak Password	May 6, 2020, 13:26:07
High	Weak password - Mysql DB login weak password baseline(Windows version)	1	Risk free	Weak Password	May 6, 2020, 13:26:07

> Note If the number in the **Failed Items/Affected Servers** column is not 0, baseline risks have been detected on your servers.

What's next

After you run a baseline check, you can view and manage detected risks on the **Baseline Check** page. For more information, see View baseline check results and handle baseline risks.

2.5. View baseline check results and handle baseline risks

After you complete a baseline check, you can view the baseline check results and handle the baseline risks that are detected on your assets on the Baseline Check page. This topic describes how to view baseline check results and handle baseline risks that are detected on your assets.

Context

After you enable the baseline check feature, Security Center runs a baseline check on all your assets based on the **default** baseline check policy. You can also create custom baseline check policies based on your business requirements. For more information about custom baseline check policies, see Create baseline check policies.

> Note

Prerequisites

A baseline check is complete. For more information, see Run a baseline check.

View baseline check results

1.
2.
3. On the **Baseline Check** page, view baseline check results.

   The Baseline Check page displays the overview of a baseline check policy and the list of baseline check results.

   - Overview of a baseline check policy
     In the upper part of the Baseline Check page, you can select a baseline check policy from the **Select Policy** drop-down list. After you select a baseline check policy from the drop-down list, the information such as **Checked Servers**, **Check Items**, **Weak Passwords**, and **Last Pass Rate** is displayed on the right. You can click **View Progress** to view the progress of the baseline check task.
     The following table describes the parameters in the upper part of the Baseline Check page.

Parameter	Description

Parameter	Description
Select Policy	The baseline check policy whose check results you want to view. You can select an existing baseline check policy from the drop-down list.
Checked Servers	The number of servers on which the baseline check runs based on the selected baseline check policy. The servers are specified in the baseline check policy.
Check Items	The number of check items specified in the selected baseline check policy.
Weak Passwords	The number of weak password risks that are detected based on the selected baseline check policy. You can click the number below **Weak Passwords** to view the list of weak password risks that are detected. **Notice** Weak password risks are of the **High** severity. We recommend that you fix the high-risk items on which weak passwords are detected at the earliest opportunity.
Last Pass Rate	The pass rate of the check items that are specified in the selected baseline check policy in the last baseline check. The following list describes the meaning of the color for the number below **Last Pass Rate**: ■ Green: high pass rate of check items. ■ Red: low pass rate of check items. We recommend that you go to the details of each check item and fix the detected baseline risks.

- List of baseline check results
  In the list of baseline check results, you can view the details of the baseline check results.

  a. In the list of baseline check results, click the name of a baseline to go to the baseline details panel.
     In the baseline details panel, view the information such as affected assets, **Passed Items** in the baseline, and **At-Risk Items** in the baseline.

  b. In the baseline details panel, find an affected asset and click **View** in the **Actions** column.
     The **At-Risk Items** panel appears.
     In the **At-Risk Items** panel, you can view all baseline risks that are detected on the asset.

  c. In the **At-Risk Items** panel, find a risk item whose details you want to view and click **Details** in the **Actions** column. In the message that appears, you can view information about the risk item, including **Description**, **Result**, and **Suggestion**.

d. (Optional)In the upper-right corner of the list of baseline check results, click the ⤓ icon. In the **Select Baseline Export Task** dialog box, select an export method and click Export to export the list of baseline check results.
   You can select one of the following export methods to export the result for the weak password baseline check:

   - **Weak password plaintext export**: exports plaintext.
   - **Weak password desensitization export**: exports the check result after the weak passwords in the result are masked.

Handle detected baseline risks

1.
2.
3. In the list of baseline check results, click the name of a baseline.
4. In the panel that appears, find a server and click **View** in the **Actions** column.
5. In the **At-Risk Items** panel, handle the baseline risks that are detected on the server.
   - **Repair**
     Security Center allows you to fix only the baseline risks that are detected on a Linux server based on the Alibaba Cloud standards or the Multi-Level Protection Scheme (MLPS) standards. If a baseline risk is detected on a Linux server based on the Alibaba Cloud standards or the MLPS standards, you can fix the baseline risk in the Security Center console. Otherwise, you must log on to the server to modify the configurations of the server on which the baseline risk is detected. After you modify the configurations, you can **verify** whether the baseline risk is fixed.
     - Fix baseline risks in the Security Center console
       a. In the **At-Risk Items** panel, find the check item based on which baseline risks are detected and click **Repair** in the **Actions** column.

b. In the **Fix Risks for Assets** dialog box, configure the parameters.
   The following table describes the parameters.

Parameter	Description
Fixing Method	The method that you use to fix a baseline risk. **Note** The method varies based on the type of the baseline risk. You can configure this parameter based on your business requirements.
Batch Handle	Specifies whether to handle the same baseline risk for multiple assets at a time.
Risk protection	Specifies whether to create snapshots for your system data. **Notice** Security Center may fail to fix baseline risks. If this issue occurs, your business may be affected. Before you fix baseline risks, we recommend that you create a backup for your system. If Security Center fails to fix the risks, you can use the backup to roll back your system to a snapshot before you fix the risks. This helps ensure that your workload runs as expected. ■ Automatically create snapshots and repair: If you select this option, configure the **Snapshot name** and **Snapshot save time** parameters and click **Fix Now**. **Note** You are charged for the usage of snapshots. You can click **View billing instructions** to view the billing methods of the snapshot service. ■ Repair directly without creating snapshot backup: If you do not want to create snapshots before you fix the baseline risks, you can click **Fix Now**.

c. Click **Fix Now**.

- Log on to a server to fix baseline risks
  In the At-Risk Items panel, find a risk item and click **Details** in the **Actions** column. In the message that appears, you can view the information about the risk item provided by Security Center. The information includes **Description**, **Result**, and **Suggestion**. Then, log on to the server on which the baseline risk is detected and modify the configurations that cause the baseline risk based on the information provided in **Suggestion**.

○ **Whitelist**

If you trust the check item whose status is **Failed**, you can add the check item to the whitelist. Then, you can ignore the alerts that are generated on the check item. After you add the check item to the whitelist, the check item is ignored. For more information, see Add a check item to the whitelist.

> ⓘ **Note** If you want to add multiple check items to the whitelist, you can select the check items and click **Whitelist** in the lower-left corner.

6. Check whether a baseline risk is fixed.

   In the **At-Risk Items** panel, find a check item and click **Verify** in the **Actions** column. Then, check whether the baseline risk on servers is fixed. If the baseline risk is fixed, the number of **At-Risk Items** decreases, and the status of the check item changes to **Passed**.

   > ⓘ **Note** If you do not perform manual verification, Security Center automatically checks whether the baseline risk is fixed based on the detection interval that is specified in your baseline check policy.

What to do next

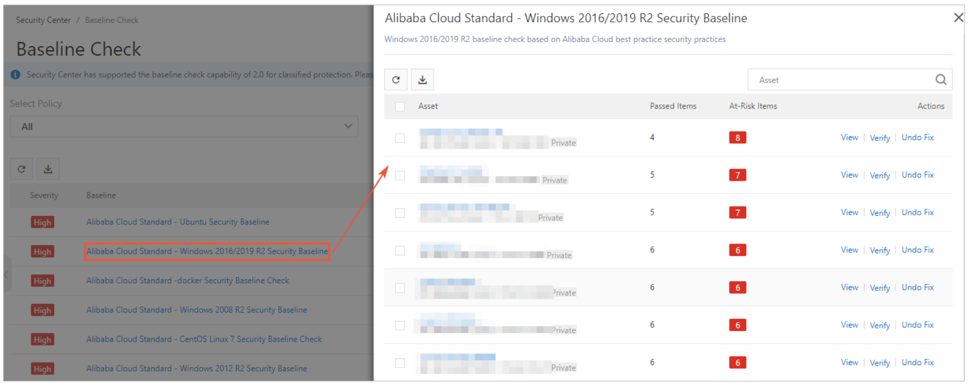
- **Rollback**
  If you want to fix baseline risks for an Elastic Compute Service (ECS) instance, we recommend that you create a snapshot for the ECS instance before the fix. This way, you can roll back the instance if a service interruption error occurs because the baseline risks failed to be fixed. To perform the rollback, you can find the instance in a baseline details panel and click **Rollback** in the **Actions** column. In the **Rollback** dialog box, select the snapshot that you created before you perform the fix and click **OK**. Then, the configurations of the instance are rolled back based on the snapshot.
- **Remove**
  If you want a check item in the whitelist to trigger alerts, you can remove the check item from the whitelist. After you remove a check item from the whitelist, the check item triggers alerts.
  In the **At-Risk Items** panel, find a check item that you want to remove from the whitelist and click **Remove** in the **Actions** column. In the **Reason for Ignore** dialog box, click **OK**. You can also remove multiple check items from the whitelist at a time. To remove multiple check items, select the check items and click **Remove** below the check item list.

2.6. Add a check item to the whitelist

You can add a check item that is provided by the baseline check feature to the whitelist. After you add a check item based on which baseline risks are detected to the whitelist, Security Center no longer generates alerts on the check item. If you trust the check item, you can add the check item to the whitelist. Then, you can ignore the alerts that are generated on the check item. This topic describes how to add a check item on which alerts are generated to the whitelist.

Procedure

1. Log on to the Security center console.
2. In the left-side navigation pane, click **Protection > Baseline Check**.
3. In the Baseline column, click the name of a baseline whose check item you want to add to the whitelist.



Security Center / Baseline Check

Baseline Check

Security Center has supported the baseline check capability of 2.0 for classified protection. Pleas

Select Policy: All

Severity	Baseline
High	Alibaba Cloud Standard - Ubuntu Security Baseline
High	Alibaba Cloud Standard - Windows 2016/2019 R2 Security Baseline
High	Alibaba Cloud Standard -docker Security Baseline Check
High	Alibaba Cloud Standard - Windows 2008 R2 Security Baseline
High	Alibaba Cloud Standard - CentOS Linux 7 Security Baseline Check
High	Alibaba Cloud Standard - Windows 2012 R2 Security Baseline

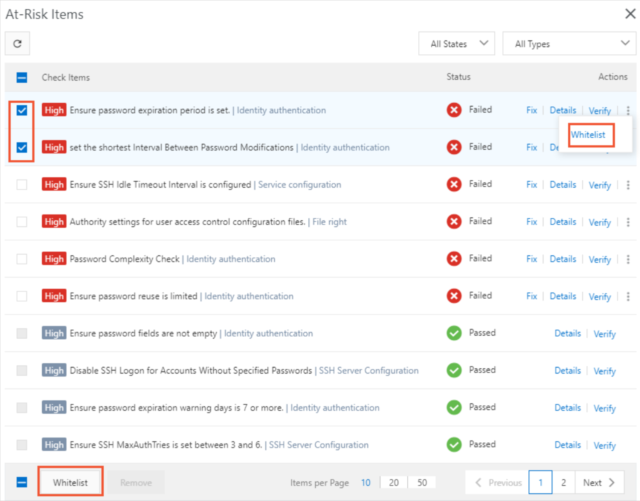
Alibaba Cloud Standard - Windows 2016/2019 R2 Security Baseline

Windows 2016/2019 R2 baseline check based on Alibaba Cloud best practice security practices

Asset	Passed Items	At-Risk Items	Actions
[redacted] Private	4	8	View | Verify | Undo Fix
[redacted] Private	5	7	View | Verify | Undo Fix
[redacted] Private	5	7	View | Verify | Undo Fix
[redacted] Private	6	6	View | Verify | Undo Fix
[redacted] rivate	6	6	View | Verify | Undo Fix
[redacted] rivate	6	6	View | Verify | Undo Fix
[redacted] Private	6	6	View | Verify | Undo Fix

4. Find the asset on which alerts are generated and click **View** in the **Actions** column to view detected baseline risks.

5. In the **At-Risk Items** panel, find the check item based on which baseline risks are detected and click **Whitelist** in the **Actions** column.

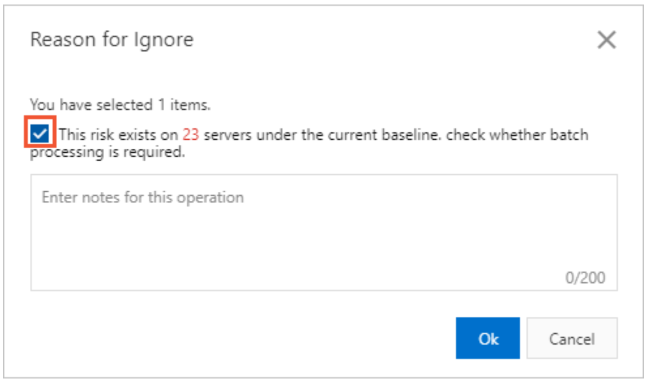


At-Risk Items

	Check Items	Status	Actions
☑	High Ensure password expiration period is set. | Identity authentication	Failed	Fix | Details | Verify | ⋮
☑	High set the shortest Interval Between Password Modifications | Identity authentication	Failed	Fix | De Whitelist
□	High Ensure SSH Idle Timeout Interval is configured | Service configuration	Failed	Fix | Details | Verify | ⋮
□	High Authority settings for user access control configuration files. | File right	Failed	Fix | Details | Verify | ⋮
□	High Password Complexity Check | Identity authentication	Failed	Fix | Details | Verify | ⋮
□	High Ensure password reuse is limited | Identity authentication	Failed	Fix | Details | Verify | ⋮
□	High Ensure password fields are not empty | Identity authentication	Passed	Details | Verify
□	High Disable SSH Logon for Accounts Without Specified Passwords | SSH Server Configuration	Passed	Details | Verify
□	High Ensure password expiration warning days is 7 or more. | Identity authentication	Passed	Details | Verify
□	High Ensure SSH MaxAuthTries is set between 3 and 6. | SSH Server Configuration	Passed	Details | Verify

To add multiple check items to the whitelist at a time, select the check items that are in the **Failed** state and click **Whitelist** in the lower-left corner.

6. In the **Reason for Ignore** dialog box, enter remarks for adding the check item to the whitelist. If you want to ignore alerts that are generated on the check item on all servers, select **check whether batch processing is required**.



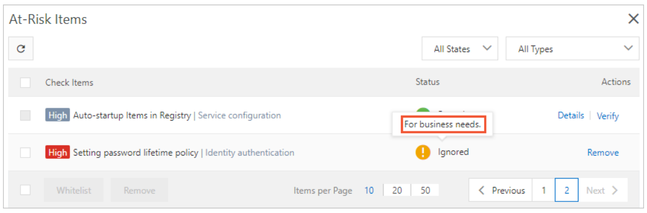
Reason for Ignore

You have selected 1 items.

☑ This risk exists on 23 servers under the current baseline. check whether batch processing is required.

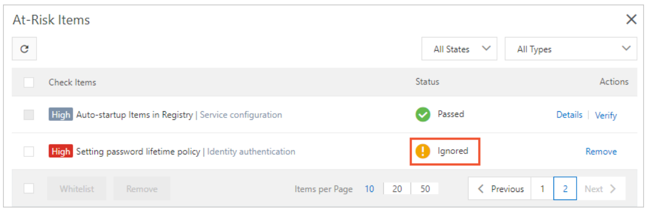
The remarks are displayed in the check item list. You can trace and analyze the check item based on the remarks.

> Note To view the remarks of a check item that is added to the whitelist, find the check item and move the pointer over **Ignored** in the Status column.



7. Click **OK**.

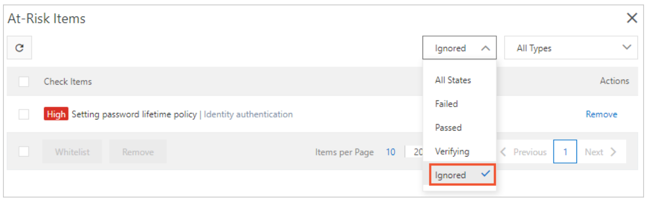
   After the check item is added to the whitelist, the check item is displayed on the last page of the check item list, and the status of the check item changes to **Ignored**.



What to do next

- View the check items that are added to the whitelist

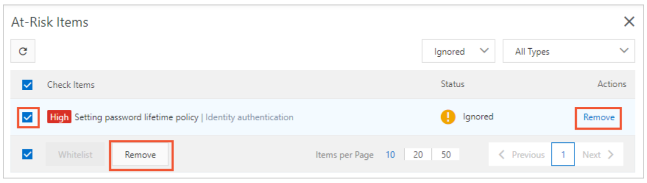
  In the **At-Risk Items** panel, select **Ignored** from the drop-down list to view the check items that are added to the whitelist.



- Remove a check item from the whitelist

  If you want to enable the alerting feature for a check item that is added to the whitelist, you can remove the check item from the whitelist.

  In the **At-Risk Items** panel, find the check item and click **Remove** in the **Actions** column. You can also select the check item and click **Remove** in the lower-left corner of the check item list. In the **Cancel ignore operation** dialog box, click **OK** to remove the check item from the whitelist.



3.Cloud platform configuration assessment

3.1. Overview

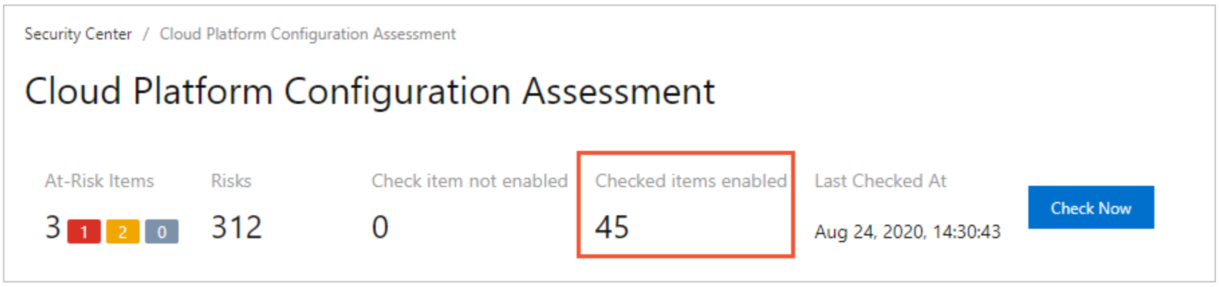
Security Center provides the configuration assessment feature to detect risks in the configurations of your Alibaba Cloud services. This topic describes the configuration assessment feature and the supported check items.

Background information

Security Center checks the following configurations of your Alibaba Cloud services to detect risks: identity authentication and permissions, network access control, data security, log audit, monitoring and alerting, and basic security protection. If risks are detected, Security Center provides solutions for the risks.

> **Note** The and editions of Security Center support a limited number of check items. The , , and editions support all check items. If you use the or edition and want to use the configuration assessment feature to check all items, upgrade Security Center to the , , or edition. For more information about the check items that each edition supports, see Check items.

You can view the number of enabled check items in **Checked items enabled** on the **Cloud Platform Configuration Assessment** page.



Security Center / Cloud Platform Configuration Assessment

Cloud Platform Configuration Assessment

At-Risk Items: 3 (1, 2, 0)

Risks: 312

Check item not enabled: 0

Checked items enabled: 45

Last Checked At: Aug 24, 2020, 14:30:43

Check items

The following table describes the check items that each edition of Security Center supports. Security Center has the following editions: , , , , and . The following symbols are used to indicate whether a check item is supported:

- ×: The check item is not supported.
- √: The check item is supported.

Check item	Type	Description	and	, , and

Check item	Type	Description	and	, , and
Alibaba Cloud account security - AccessKey pair	Identity authentication and permissions	Checks the AccessKey pair of your Alibaba Cloud account. Your Alibaba Cloud account has full permissions on your resources. To prevent the loss caused by AccessKey pair leaks, we recommend that you do not create an AccessKey pair for your Alibaba Cloud account or use the AccessKey pair in day-to-day operations. **Notice** The results of this check are delayed. If you disable the AccessKey pair, the results of the check are updated on the following day.	×	√
Alibaba Cloud CDN - real-time log push feature	Log audit	Checks whether the real-time log push feature is enabled for Alibaba Cloud CDN. Alibaba Cloud CDN is integrated with Log Service to deliver log data to Log Service in real time. You can analyze real-time logs to identify and locate issues.	×	√
PolarDB - backup configurations	Data security	Checks whether the automatic backup feature is enabled for PolarDB. Database backups reinforce security and allow you to restore data when an error occurs in your database. PolarDB provides the automatic backup feature. We recommend that you enable the automatic backup feature to create a backup on a daily basis.	×	√
PolarDB - SQL Explorer	Log audit	Checks whether the SQL Explorer feature is enabled for PolarDB. PolarDB supports the SQL Explorer feature. This feature provides value-added capabilities, such as security audit and performance diagnosis. We recommend that you enable the SQL Explorer feature.	×	√

Check item	Type	Description	and	, , and
OSS - authorization policies	Identity authentication and permissions	Checks the authorization policies of Object Storage Service (OSS). OSS supports three types of access control policies: access control lists (ACLs), Resource Access Management (RAM) policies, and bucket policies. When you configure bucket policies, we recommend that you do not grant the read and write permissions or full permissions to anonymous users.	×	√
SLB - logging	Log audit	Checks whether the logging feature is enabled for Server Load Balancer (SLB). SLB provides the logging feature that records Layer 7 requests. This feature collects details about requests that are sent to SLB. The details include the request time, client IP address, network latency, request path, and server response. We recommend that you enable the logging feature.	×	√
Container Registry - repository permission configurations	Data security	Checks whether a Container Registry repository is set to private. Container Registry supports public and private repositories. Public repositories allow anonymous users to download images over the Internet. If images in a repository contain sensitive information, we recommend that you set the repository to private.	×	√
Container Registry - security scans	Basic security protection	Checks whether the security scan feature is enabled for Container Registry. Container Registry supports security scans for Linux base images. Security scans can detect system vulnerabilities and risks in base images. We recommend that you scan all images. If new versions of the base images are obtained, we recommend that you perform security scans on the new versions.	×	√
ECS - security group policies	Network access control	Checks the policies of Elastic Compute Service (ECS) security groups. We recommend that you grant minimum permissions to users. If you set 0.0.0.0/0 for a service, requests from all IP addresses are allowed. For example, you can set 0.0.0.0/0 for port 80, 443, 22, or 3389.	×	√

Check item	Type	Description	and	, , and
OSS - bucket server-side encryption	Data security	Checks whether the data encryption feature is enabled for OSS buckets. OSS supports server-side encryption to ensure the security of data that is persistently stored in OSS. We recommend that you enable server-side encryption to protect sensitive data.	×	√
OSS - bucket hotlink protection	Network access control	Checks whether the hotlink protection feature is enabled for OSS buckets. The OSS hotlink protection feature checks the Referer header to deny access from unauthorized users. We recommend that you enable this feature.	×	√
ApsaraDB RDS - cross-region backup configurations	Data security	Checks whether the cross-region backup feature is enabled for ApsaraDB RDS instances. ApsaraDB RDS for MySQL provides the cross-region backup feature. This feature automatically synchronizes on-premises backup files to OSS buckets in another region. This implements geo-disaster recovery. We recommend that you enable the cross-region backup feature.	×	√
ApsaraDB for Redis - backup configurations	Data security	Checks whether the data backup feature is enabled for ApsaraDB for Redis instances.	×	√
ApsaraDB for Redis - SSL encryption	Log audit	Checks whether SSL encryption is enabled for ApsaraDB for Redis instances. ApsaraDB for Redis 2.8 standard master-replica instances, ApsaraDB for Redis 2.8 master-replica cluster instances, and ApsaraDB for Redis 4.0 master-replica cluster instances support SSL encryption. We recommend that you enable SSL encryption to reinforce the security of data in transit.	×	√
ApsaraDB for MongoDB - log audit	Log audit	Checks whether the log audit feature is enabled for ApsaraDB for MongoDB instances. This feature records all operations that you perform on the databases of ApsaraDB for MongoDB instances. Log audit helps you perform fault analysis, behavior analysis, and security audit on the databases. You can also obtain the information about data consumption. We recommend that you enable the log audit feature for ApsaraDB for MongoDB instances.	×	√

Check item	Type	Description	and	, , and
ApsaraDB for MongoDB - SSL encryption	Data security	Checks whether SSL encryption is enabled for ApsaraDB for MongoDB instances. We recommend that you enable the SSL encryption feature to reinforce the security of ApsaraDB for MongoDB instances.	×	√
ApsaraDB for MongoDB - backup configurations	Data security	Checks whether the automatic backup feature is enabled for ApsaraDB for MongoDB instances. Database backups reinforce security and allow you to restore data when an error occurs in your database. ApsaraDB for MongoDB provides the automatic backup feature. We recommend that you enable the automatic backup feature to create a backup on a daily basis.	×	√
CloudMonitor - agent status	Monitoring and alerting	Checks the status of ECS instances. CloudMonitor helps you monitor Alibaba Cloud resources and web applications. To monitor the status of ECS instances and send alerts when exceptions occur, we recommend that you install the CloudMonitor agent on your ECS instances.	×	√
VPC - DNAT management port mapping	Network access control	Checks whether a port is open to the Internet. When you create a destination network address translation (DNAT) rule for a Network Address Translation (NAT) gateway deployed in a virtual private cloud (VPC), we recommend that you do not open internal management ports to the Internet. Do not open all ports or important ports, such as port 22, 80, 443, 1433, 3306, 3389, or 8080, to the Internet.	×	√

Check item	Type	Description	and	, , and
Alibaba Cloud - two-factor authentication	Identity authentication and permissions for Alibaba Cloud accounts	Checks whether two-factor authentication is enabled for your Alibaba Cloud account. If you use only password authentication, attackers may use methods such as brute-force attacks to obtain the password to your Alibaba Cloud account. We recommend that you enable two-factor authentication that requires both password and SMS verification to prevent the loss caused by password leaks.	√	√
RAM users - MFA	Identity authentication and permissions for RAM users	Checks whether multi-factor authentication (MFA) is enabled for RAM users.	√	√
Alibaba Cloud Security - agent status	Basic security protection	Checks the installation of the Server Guard agent. You must install the Server Guard agent on your servers before Server Guard can protect your servers. If the Server Guard agent is not installed on your servers, your servers are vulnerable to risks, such as webshells, trojans, remote logons, and brute-force attacks.	√	√
Alibaba Cloud Security - back-to-origin configuration checks for Anti-DDoS Pro or Anti-DDoS Premium	Network access control	Checks whether Anti-DDoS Pro or Anti-DDoS Premium allows requests from only Web Application Firewall (WAF) back-to-origin IP addresses. After you use Anti-DDoS Pro, Anti-DDoS Premium, or WAF, we recommend that you hide the IP address of the origin server to prevent attacks.	√	√
Alibaba Cloud Security - back-to-origin configuration checks for WAF	Network access control	Checks whether WAF allows requests from only WAF back-to-origin IP addresses. After you use Anti-DDoS Pro, Anti-DDoS Premium, or WAF, we recommend that you hide the IP address of the origin server to prevent attacks.	√	√
Security Center - detection of AccessKey pair leaks	Monitoring and alerting	Checks whether the AccessKey pair leak detection and account security features of Security Center are enabled.	√	√

Check item	Type	Description	and	, , and
ECS - public key authentication	Identity authentication and permissions	Checks whether ECS instances that run Linux operating systems are associated with Alibaba Cloud SSH key pairs. SSH public key authentication is more secure and convenient than SSH password authentication. We recommend that you use SSH public key authentication.	√	√
ECS - storage encryption	Data security	Checks whether encryption is enabled for disks on ECS instances.	√	√
ECS - automatic snapshot policies	Data security	Checks whether the automatic snapshot feature is enabled for ECS instances. The automatic snapshot feature reinforces the security of ECS instances and supports disaster recovery.	√	√
SLB - whitelist configurations	Network access control	Checks the access control configurations of SLB instances. The configurations include whether access control is enabled for HTTP and HTTPS services and whether 0.0.0.0/0 is added to the IP address whitelist.	√	√
SLB - open ports	Network access control	Checks whether ports of SLB instances are unnecessarily open to the Internet.	√	√
SLB - health status	Monitoring and alerting	Checks whether SLB backend servers are available.	√	√
SLB - certificate validity checks	Monitoring and alerting	Checks whether your SLB certificate expires.	√	√
OSS - bucket permissions	Data security	Checks whether the OSS bucket ACL is set to **private**.	√	√
OSS - logging	Data security	Checks whether the logging feature is enabled for OSS.	√	√
OSS - cross-region replication	Data security	Checks whether the cross-region replication feature is enabled for OSS.	√	√
ApsaraDB RDS - whitelist configurations	Network access control	Checks whether a whitelist is configured for ApsaraDB RDS and whether the whitelist contains 0.0.0.0/0. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.	√	√

Check item	Type	Description	and	, , and
ApsaraDB RDS - database security policies	Data security	Checks whether the SQL audit, SSL encrypted transmission, and transparent database encryption features are enabled for ApsaraDB RDS instances.	√	√
ApsaraDB RDS - database backup	Data security	Checks whether the database backup feature is enabled for ApsaraDB RDS instances.	√	√
ApsaraDB for Redis - whitelist configurations	Network access control	Checks whether a whitelist is configured for ApsaraDB for Redis and whether the whitelist contains 0.0.0.0/0. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.	√	√
AnalyticDB for PostgreSQL - whitelist configurations	Network access control	Checks whether a whitelist is configured for AnalyticDB for PostgreSQL and whether the whitelist contains 0.0.0.0/0. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.	√	√
SSL Certificates Service - validity checks	Data security	Checks whether your SSL certificate expires. If your SSL certificate expires, you are not allowed to use the certificate.	√	√
PolarDB - whitelist configurations	Network access control	Checks whether a whitelist is configured for PolarDB and whether the whitelist contains `0.0.0.0/0`. If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.	√	√
ActionTrail - logging	Log audit	Checks operation logs in OSS or Log Service. To trace high-risk operations, we recommend that you activate ActionTrail, store operation logs in OSS or Log Service, and set proper access permissions.	√	√

Check item	Type	Description	and	, , and
ApsaraDB for MongoDB - whitelist configurations	Network access control	Checks whether a whitelist is configured for ApsaraDB for MongoDB and whether the whitelist contains `0.0.0.0/0` . If the whitelist contains 0.0.0.0/0, requests from all IP addresses are allowed. We recommend that you configure the whitelist to allow requests only from specific IP addresses.	√	√
Apsara Devops - Codeup security	Basic security protection	Checks the status of code in Codeup and analyzes whether the code is secure from the following aspects: access control, member behavior, and code content. Codeup provides suggestions on security configurations based on the check results.	√	√
RAM - excessive authorization	Identity authentication and permissions	If you want to grant permissions to a RAM user, a RAM user group, or a RAM role, follow the principle of least privilege. This prevents excessive authorizations. The following list describes the principals that can be checked by using the check item: • The principal to which the AdministratorAccess policy is attached. • The principal to which a custom policy is attached. The custom policy grants all permissions on all resources.	X	√
OSS - bucket versioning	Data security	OSS allows you to configure versioning for a bucket to protect objects that are stored in the bucket. After you enable versioning for a bucket, data that is overwritten or deleted in the bucket is saved as a previous version. After you configure versioning for a bucket, you can recover objects in the bucket to any previous version to protect your data from being accidentally overwritten or deleted.	×	√

Related information

- Perform configuration checks on cloud services
- View the check results of configuration assessment for your cloud services and handle the detected risks

3.2. Perform configuration checks on cloud services

The configuration assessment feature allows you to manually run configuration checks and enable automatic checks on your cloud services. This topic describes how to manually run configuration checks on your cloud services and how to specify a detection cycle for automatic checks.

Context

You can use the configuration assessment feature to manually run configuration checks on your cloud services. You can also use the feature to specify a detection cycle for automatic checks. The feature helps you monitor the security status of your cloud services and handle detected risks at the earliest opportunity.

Manual checks

If you want to immediately check whether the configurations of your cloud services contain risks, perform the following operations to run manual checks:

1.
2.
3. On the **Cloud Platform Configuration Assessment** page, click **Scan now** to check whether the configurations of all your cloud services contain risks and obtain the number of affected assets.

   > ? Note Wait until the configuration check on all cloud services is complete.

Automatic checks

By default, Security Center automatically runs configuration checks during `24:00 - 06:00` every two days. If the default configurations for automatic checks do not meet your business requirements, you can specify the detection cycle and time for automatic checks.

1.
2.
3.
4. In the **Settings** panel, configure the Detection Cycle, Detection Time, and Risk Check Item parameters.
5. Click **OK**.
   Security Center automatically runs checks against the selected check items based on the detection cycle and time that you specify.

What's next

After the check is complete, you can go to the **Cloud Platform Configuration Assessment** page to view the check results and handle the detected risks. For more information, see View the check results of configuration assessment for your cloud services and handle the detected risks.

3.3. View the check results of configuration assessment for your cloud services and handle the detected risks

You can handle the detected configuration risks on the Cloud Platform Configuration Assessment page in a centralized manner. This topic describes how to view the check results of configuration assessment for your cloud services. This topic also describes how to handle the configuration risks that are detected on your cloud services.

Context

For more information about the configuration risks that can be detected by Security Center, see Check items.

Prerequisites

Configuration checks are run on your cloud services. For more information, see Perform configuration checks on cloud services.

View check results

1.
2.
3. On the **Cloud Service Check** page, view the check results of configuration assessment for your cloud services.

   You can perform the following operations:

   - View the overall information
     The section in the upper part of the **Cloud Platform Configuration Assessment** page displays the overall information. You can view the pass rate of check items in **Pass Rate**. You can move the pointer over the lines below **Pass Rate** to view the numbers of check items at different severity levels. The red line indicates **high-risk** items, the orange line indicates **medium-risk** items, the blue line indicates **low-risk** items, and the green line indicates **passed** check items.
   - View risk items
     - You can click a type of best security practice in the **All Check Items** section. In the list of check items, view the check items that are related to the security best practice.

    - You can also use the filters above the list to search for check items that you want to view. The filter conditions include the severity level and the status of check items.

    > **Note** Lines in different colors indicate different severity levels. The following list describes the mappings between the colors and the severity levels:
    >
    > - **Important**: red. The risk item poses major threats to your assets. We recommend that you handle the risk item at the earliest opportunity.
    > - **Medium**: orange. The risk item causes damage to your assets. You can handle the risk item at your convenience.
    > - **Low**: gray. The risk item causes less damage to your assets. You can handle the risk item at your convenience.

- View details of a risk item
  Find a risk item and click the name of the risk item or **Details** in the **Operate** column. In the details panel of the risk item, you can view the following information: **Check Item Description**, **Solution**, and **Reference**.

Handle the detected configuration risks of your cloud services

1.
2.
3. On the **Cloud Platform Configuration Assessment** page, handle the detected configuration risks of your cloud services.

   You can perform the following operations based on your business requirements:

   - Fix risks
     In the **Risks** section of the details panel of a risk item, click the instance ID of the cloud service on which risks are detected to go to the console of the cloud service. Then, fix the risks in the cloud service based on the information provided in the **Solution** and **Reference** sections of the details panel of the risk item.
   - Verify the fixing of risks
     - If you have modified the configuration of an instance based on the information provided in the details panel of a risk item that affects the instance, you can find the instance and click **Verify** in the **Operate** column to check whether the new configuration contains risks. If the configuration does not contain risks, the instance is removed from the list in the **Risks** section.
     - If you have modified the configurations of all instances that are affected by the risk item, you can find the risk item in the check item list on the **Cloud Platform Configuration Assessment** page and click **Verify** in the **Operate** column to check whether the new configurations contain risks. If no configurations contain risks, the status of the risk item changes to **Passed**.
     - If you want to verify the fixing of multiple risk items, select the risk items and click **Verify** below the check item list. In the message that appears, click **OK**.
   - Add a risk item to the whitelist
     If you identify a risk item as a false positive, you can find the risk item in the check item list on the **Cloud Platform Configuration Assessment** page and click **Whitelist** in the **Operate** column to add the risk item to the whitelist. The status of the risk item changes to **Whitelist**. Risk items that are in the **Whitelist** state are not counted in the total number of risk items.

> **Note** After you add a risk item to the whitelist, the risks that are detected for the risk item are no longer reported in subsequent configuration checks. We recommend that you do not add risk items to the whitelist unless necessary.

You can remove a risk item from the whitelist. To remove a risk item from the whitelist, find the risk item in the check item list on the **Cloud Platform Configuration Assessment** page and click **Remove** in the Operate column.

4.Image security scans

4.1. Overview

The feature of container image scan detects and identifies high-risk system vulnerabilities, application vulnerabilities, malicious samples, configuration risks, and sensitive data in images. It also provides suggestions on how to handle these issues and end-to-end vulnerability management. This makes image vulnerability fixes easier.

Background information

Container image scan is a value-added feature of Security Center and must be separately purchased. Only users of the ,, , and editions can purchase container image scan.

> **Note** Users of the edition can upgrade Security Center to the , , , or edition to purchase container image scan. Users of the edition can upgrade Security Center to the , , or edition to purchase container image scan.

Supported regions

Only the Container Registry instances in the following regions support container image scan: China (Hangzhou), China (Shanghai), China (Beijing), China (Shenzhen), China (Hong Kong), and Singapore (Singapore).

Items that can be detected

Item	Detection	Fixing	Remarks
Image system vulnerability	Supported	Supported	We recommend that you fix image system vulnerabilities at the earliest opportunity based on the fixing commands and impact descriptions provided by Security Center.
Image application vulnerability	Supported	Not supported	We recommend that you fix image application vulnerabilities at the earliest opportunity based on the fixing commands and impact descriptions provided by Security Center.
Image baseline risk	Supported	Not supported	We recommend that you handle image baseline risks at the earliest opportunity based on the baseline check details provided by Security Center.
Malicious image sample	Supported	Not supported	We recommend that you handle malicious file samples at the earliest opportunity based on the information provided by Security Center. The information includes paths to malicious files.

Supported operating systems and versions

Operating system	Version
Red Hat	5, 6, and 7
CentOS	5, 6, and 7
Ubuntu	12.04, 14.04, 16.04, 18.04, and 18.10
Debian	6, 7, 8, 9, and 10
Alpine	• 2.3, 2.4, 2.5, 2.6, and 2.7 • 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, and 3.12
Amazon Linux	• Amazon Linux 2 • Amazon linux AMI
Oracle Linux	5, 6, 7, and 8
SUSE Linux Enterprise Server	• 5, 6, 7, 8, 9, and 10 • 10 SP4 • 11 SP3 • 12 SP2 • 12 SP5
Fedora Linux	2X and 3X
openSUSE	• 10.0 • Leap 15.2 • Leap 42.3

References

View security information about containers

Use threat detection on Kubernetes containers

Use the runtime security feature to monitor ACK clusters and configure alerts

4.2. Enable container image scan

To use the feature of container image scan, you must purchase and enable this feature. This topic describes how to purchase and enable container image scan.

Context

Container image scan is a value-added feature of Security Center and must be separately purchased. Only users of the ,, , and editions can purchase container image scan.

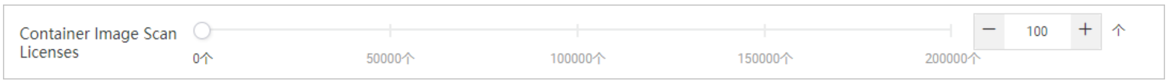
If you purchase container image scan, you are charged base on the quota specified by Container Image Scan. For more information about billing details, visit .

Note Users of the edition can upgrade Security Center to the , , , or edition to purchase container image scan. Users of the edition can upgrade Security Center to the , , or edition to purchase container image scan.

Procedure for users of Security Center

1.
2.
3. On the page that appears, click **Immediate purchase**.
4. Click **Buy Advanced**, **Buy Enterprise**, or **Buy Ultimate Edition**.

   In addition to all the features that the **Enterprise** edition supports, the **Ultimate** edition also supports **network topology of containers**, **threat detection for Kubernetes containers**, and **threat detection during container runtime**. If you have high requirements for container security, we recommend that you click **Buy Ultimate Edition**. For more information about the features that each edition supports, see Features.
5. After you click **Buy Advanced**, **Buy Enterprise**, or **Buy Ultimate Edition**, configure the parameters, including **Container Image Scan**.

   Container Image Scan Licenses: 100

   We recommend that you set **Container Image Scan** to the number of images for which you want to detect container vulnerabilities during the subscription period. Security Center identifies an image based on a unique digest value. If the digest value of an image does not change, the quota specified by Container Image Scan is deducted only by one from the first scan. If the digest value of an image changes and the image is scanned again, the quota specified by Container Image Scan is deducted again. The quota is deducted by one each time the digest value changes. For example, if you want to scan 10 images and the total number of times the digest values of the images change is expected to be 20 within the subscription period, set **Container Image Scan** to 30. This indicates that the value of Container Image Scan equals the number of images you want to scan plus the number of times the digest values change.
   References:

   - For more information about the billing details, see Billing.
   - For more information about how to configure the parameters on the buy page, see Purchase Security Center.

   Note If you want to use only container image scan of Security Center, you can set Edition to and **Container Image Scan** to an appropriate value.
6. Click **Buy Now** and complete the payment.

Procedure for users of all paid editions

If you use Security Center , you must upgrade Security Center to the , , or edition and specify Container Image Scan before you can enable container image scan. If you use the , , or edition of Security Center, you must specify Container Image Scan before you can enable container image scan. For more information, see Upgrade and downgrade Security Center.

4.3. Add image repositories to Security Center

Before you can use Security Center to scan images, you must add an image repository to Security Center. This topic describes how to add image repositories to Security Center.

Prerequisites

The feature of container image scan is enabled. For more information, see Enable container image scan.

Image repositories that can be added to Security Center

The following types of image repositories can be added to Security Center:

- Image repositories of Container Registry
- Third-party image repositories: Harbor repositories and Quay repositories

Add an image repository of Container Registry to Security Center

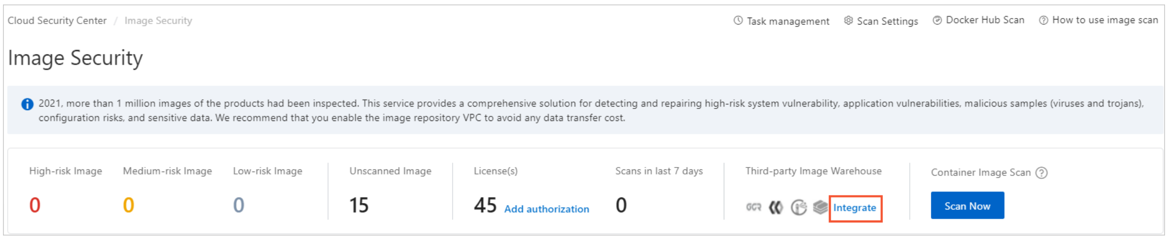
Container Registry has Enterprise Edition and Personal Edition. You can synchronize the information about the images in the image repositories of both Container Registry Enterprise Edition and Container Registry Personal Edition to Security Center. However, Security Center can scan the images only of Container Registry Enterprise Edition.

After you configure access to a Container Registry Enterprise Edition instance over a virtual private cloud (VPC), the image repositories of the instance are added to Security Center. For more information, see Configure access over VPCs.

Add a third-party image repository deployed on a public cloud to Security Center

If your third-party image repository is deployed on a public cloud, perform the following steps to add the image repository to Security Center:

1.
2.
3. On the **Image Security** page, click **Integrate** in the **Third-party Image Warehouse** section.



2021, more than 1 million images of the products had been inspected. This service provides a comprehensive solution for detecting and repairing high-risk system vulnerability, application vulnerabilities, malicious samples (viruses and trojans), configuration risks, and sensitive data. We recommend that you enable the image repository VPC to avoid any data transfer cost.

High-risk Image	Medium-risk Image	Low-risk Image	Unscanned Image	License(s)	Scans in last 7 days	Third-party Image Warehouse	Container Image Scan
0	0	0	15	45 Add authorization	0	Integrate	Scan Now

4. In the **Integrate image repository** panel, configure the parameters.

   The following table describes the parameters.

Parameter	Description

Parameter	Description
Private repository type	The type of the third-party image repository. Valid values: **harbor** and **quay**. **Note** Specify Private repository type based on the type of your image repository.
Version	The version of the third-party image repository. Valid values: ○ **V1**: If the version of the image repository is 1.X.X, select this option. ○ **V2**: If the version of the image repository is 2.X.X or later, select this option.
Communication Type	The protocol that you want Security Center to use to communicate with the third-party image repository. Valid values: **http** and **https**.
Network Type	The network type of the third-party image repository. Valid values: **Public** and **VPC**.
RegionId	The ID of the region in which the third-party image repository resides.
IP	The IP address of the third-party image repository. **Note** If the third-party image repository is deployed on a hybrid cloud, you must configure the **IP** parameter.
Domain	The domain name of the third-party image repository.
Speed limit	The number of images that can be added to Security Center per hour. Default value: **10**. Valid values: ○ **5** ○ **10** ○ **30** ○ **50** ○ **200** ○ **500** ○ **1000** ○ **Unlimited** **Notice** If you add a large number of images per hour, your services may be adversely affected. In most cases, we recommend that you do not set this parameter to **Unlimited**.

Parameter	Description
Username	The username used to access the third-party image repository.
Password	The password used to access the third-party image repository.

5. Click **Next**.
   The third-party image repository is added to Security Center. Then, you can click **Scan Settings** on the **Image Security** page to view the information about the added image repository in the panel that appears.

Add a third-party image repository deployed on a hybrid cloud to Security Center

If your third-party image repository is deployed on a hybrid cloud that is composed of VPCs and data centers, you must configure traffic forwarding rules and then add the image repository to Security Center. To add the image repository, perform the following steps:

1. Specify an ECS instance and configure traffic forwarding rules to forward the traffic destined for the ECS instance to an on-premises server on which the third-party image repository resides.

   In the following command examples, the traffic on Port A of the ECS instance is forwarded to Port B of the on-premises server that uses the IP address of 192.168.XX.XX.

   - Command examples for CentOS 7
     - Use firewall-cmd:

       ```
       firewall-cmd --permanent --add-forward-port=port=<Port A>:proto=tcp:toaddr=<192.168
       .XX.XX>:toport=<Port B>
       ```

     - Use iptables:

       a. Enable port forwarding.

       ```
       # echo "1" > /proc/sys/net/ipv4/ip_forward
       ```

       b. Configure port forwarding.

       ```
       # iptables -t nat -A PREROUTING -p tcp --dport <Port A> -j DNAT --to-destinatio
       n <192.168.XX.XX>:<Port B>
       ```

   - Command example for Windows

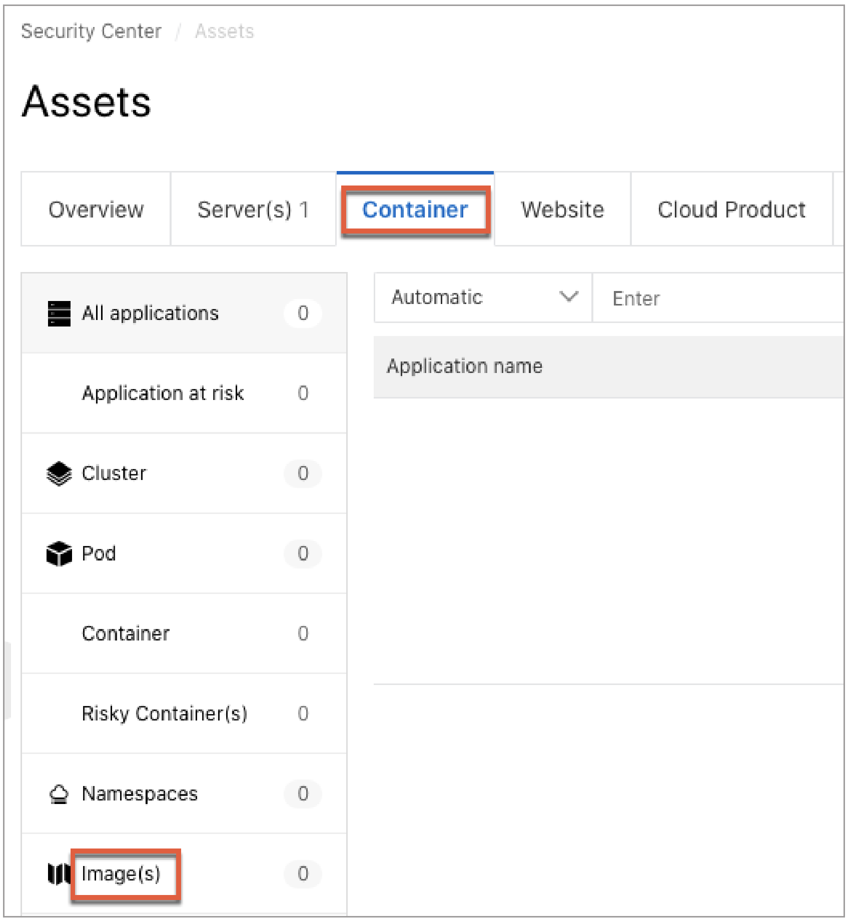
     ```
     netsh interface portproxy add v4tov4 listenport=<Port A> listenaddress=* connectaddre
     ss=<192.168.XX.XX> connectport=<Port B> protocol=tcp
     ```

2. Add the third-party image repository to Security Center.

   Make sure that you set **IP** to the CIDR block of the vSwitch within the VPC for which you configured forwarding rules. For more information, see Add a third-party image repository deployed on a public cloud to Security Center.

What to do next

You can view the information about the images that are protected by Security Center on the **Assets** page.



4.4. Scan images

Security Center provides the feature of container image scan. You can use the feature to check whether vulnerabilities and malicious samples exist in your images. This helps ensure a secure runtime environment for your images. This topic describes how to scan images.

Prerequisites

- A Container Registry Enterprise Edition instance is purchased or a third-party image repository is added to Security Center. For more information, see Create a Container Registry Enterprise Edition instance and Add image repositories to Security Center.
-
- **Container Image Scan** is set to an appropriate value.

Context

Vulnerabilities may exist in the basic system software, middleware, web applications, and databases that are in your images. The vulnerabilities include mining trojans and backdoor programs, which pose threats to your assets. Security Center allows you to immediately scan images or configure a cycle to scan for image vulnerabilities. For more information, see Immediately scan images and Configure a cycle to scan for image vulnerabilities.

Notice If your images have been changed, the number of times specified by **Container Image Scan** is deducted when you scan images. An image is considered changed when the digest value of the image changes. Before you scan images, make sure that **Container Image Scan** is set to an appropriate value.

Immediately scan images

To immediately scan images, click **Scan Now** on the **Image Security** page. In the **One-Click Scan** dialog box, select the type of the images that you want to scan and click **OK**. The following types of image repositories can be scanned:

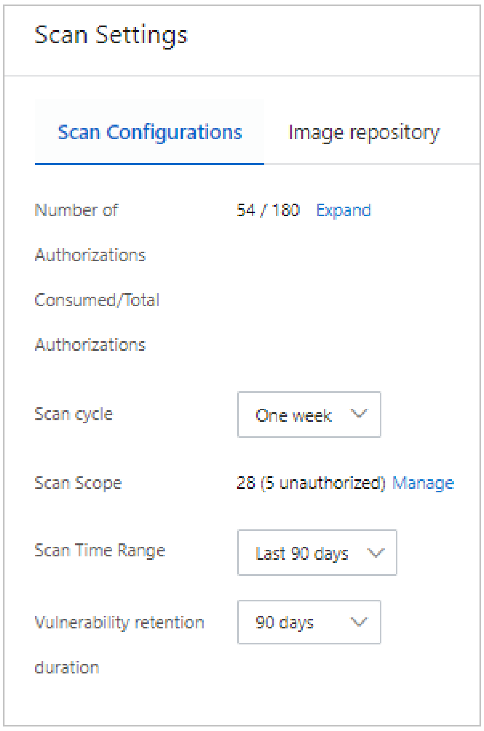
- **ACR**: If you select acr in the dialog box, Security Center checks whether vulnerabilities and malicious samples exist in your Container Registry Enterprise Edition instance that is created in the Container Registry console.
- **Harbor**: If you select harbor in the dialog box, Security Center checks whether vulnerabilities and malicious samples exist in the Harbor image repositories that you added to Security Center.

The scan takes approximately 1 minute. You can refresh the Image security scan tab and view the scan results in the list of image vulnerabilities after 1 minute.

Configure a cycle to scan for image vulnerabilities

To scan your assets for image vulnerabilities and malicious samples on a regular basis, perform the following operations to configure a scan cycle:

1.
2.
3. In the upper-right corner of the **Image Security** page, click **Scan Settings**.
4. In the **Scan Settings** panel, configure the parameters.



Scan Settings

Number of Authorizations Consumed/Total Authorizations 54 / 180 Expand

Scan cycle: One week

Scan Scope: 28 (5 unauthorized) Manage

Scan Time Range: Last 90 days

Vulnerability retention duration: 90 days

The following table describes the parameters.

Parameter	Description
Number of Authorizations Consumed/Total Authorizations	The number of image scans that are performed and the total number of image scans that are allowed. If the number of image scans that are allowed is about to be used up, you can click **Expand** to specify Container Image Scan on the Upgrade/Downgrade page based on your business requirements.
Scan cycle	The cycle at which you want to scan your images. Valid values: ○ **3 Days** ○ **One week** ○ **Two weeks** ○ **Stop**
Scan Scope	The scope of images that you want to scan. To select the scope, perform the following steps: i. Click **Manage** on the right of **Scan Scope**. ii. In the **Image management** dialog box, select the image repository that you want to scan. iii. Click **OK**.
Scan Time Range	The period in which you want to scan for image vulnerabilities. Valid values: ○ **Last day** ○ **Last 3 days** ○ **Last 7 days** ○ **Last 15 days** ○ **Last 20 days** ○ **Last 90 days** ○ **Last 180 days** ○ **Last 365 days**
Vulnerability retention duration	The retention period for detected vulnerabilities. The detected vulnerabilities are deleted after the specified retention period. Valid values: ○ **30 days** ○ **60 days** ○ **90 days** ○ **180 days**

After the parameters are configured, Security Center scans your images based on the configurations.

Manage image repositories

You can click the **Image repository** tab in the Scan Settings panel to view the Container Registry Enterprise Edition instances that support container image scan and the third-party image repositories that you added to Security Center. The Container Registry instances use the image repositories of the **ACR** type. The third-party image repositories are of the **Harbor** type.

> ? **Note** Security Center automatically adds Container Registry Enterprise Edition instances within your account to the image repository list. You cannot remove the Container Registry Enterprise Edition instances from the image repository list.

- If you want to scan the third-party image repositories that are not displayed on the Image repository tab, you can click **Integrate image repository** to go to the Integrate image repository panel and add your third-party image repositories to Security Center. For more information about the parameters in the **Integrate image repository** panel, see Add image repositories to Security Center.
- If you do not want to scan a third-party image repository that is displayed on the Image repository tab, you can click **Remove** in the **Operation** column for the image repository. In the message that appears, click **OK** to remove the image repository.

  > ? **Note** The default image repositories that are displayed on the image repository tab cannot be deleted. The types of the default image repositories are acr and defaultAcr.

Configure baseline checks for images

After you configure a cycle to scan your images for vulnerabilities, you can also configure baseline checks for the images.

1.
2.
3. In the upper-right corner of the **Image Security** page, click **Scan Settings**.
4. In the **Scan Settings** panel, click the **Baseline Configuration Management** tab.
5. Click **Management** to the right of **Configuration Scope**.
6. In the **Baseline check scope** panel, select the baselines that you want to check.

   > **Notice** The baselines that are specified for the **Accesskey Leakage Detection** and **Password leakage check** parameters below Configuration Scope are the same as those in the **Access Key Leakage** and **Password leakage** sections in the **Baseline check scope** panel. If you select baselines in the **Access Key Leakage** and **Password leakage** sections in the **Baseline check scope** panel, the switches for the **Accesskey Leakage Detection** and **Password leakage check** parameters below Configuration Scope are turned on. You do not need to configure these parameters. You can also turn on or off the switches for the **Accesskey Leakage Detection** and **Password leakage check** parameters to enable or disable the baseline checks.

7. In the lower-part of the panel, click **OK**.
   After the configurations are complete, Security Center scans your images and checks the baselines of the images.

What's next

After Security Center scans your images, you can view the scan results. For more information, see View image scan results.

4.5. View image scan results

Security Center provides the feature of container image scan to detect system vulnerabilities, application vulnerabilities, baseline risks, and malicious image samples in your images, and displays the detected risks by category. This way, you can view the overall security status of your images. This topic describes how to view the risks in your images.

Prerequisites

Container image scans are performed. For more information, see Scan images.

Context

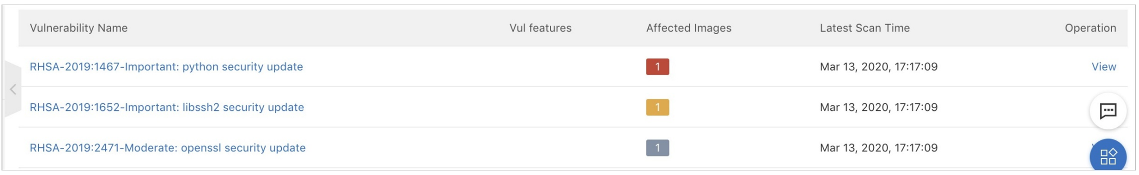
You can use container image scan to detect only image system vulnerabilities, image application vulnerabilities, baseline risks, and malicious image samples. You cannot use this feature to fix the vulnerabilities. We recommend that you handle risks in containers at the earliest opportunity based on the information provided by Security Center. The information includes fixing commands, impact descriptions, and paths to malicious files.

View image system vulnerabilities

1.
2.
3. On the **Image Security** page, click the **Image System Vul** tab.
4. On the **Image System Vul** tab, view the detected image system vulnerabilities.

   You can perform the following operations:

   - **View vulnerabilities**
     View the vulnerability names, vulnerability characteristics, number of affected images, and last scan time.
   - **View vulnerability priorities**
     The priorities of vulnerabilities are displayed in different colors in the Affected Assets column. The number in each row of the column indicates the total number of the assets affected by a vulnerability. The following list describes the relationship between colors and priorities:
     - Red: **High**
     - Orange: **Medium**
     - Gray: **Low**



Vulnerability Name	Vul features	Affected Images	Latest Scan Time	Operation
RHSA-2019:1467-Important: python security update		1	Mar 13, 2020, 17:17:09	View
RHSA-2019:1652-Important: libssh2 security update		1	Mar 13, 2020, 17:17:09	
RHSA-2019:2471-Moderate: openssl security update		1	Mar 13, 2020, 17:17:09	

> **Note** We recommend that you fix the vulnerabilities that have the **High** priority at the earliest opportunity.

   - **Search for vulnerabilities**
     On the **Image System Vul** tab, filter vulnerabilities by vulnerability priority, instance ID, repository name, namespace, digest, or vulnerability name. A vulnerability priority can be high, medium, or low.

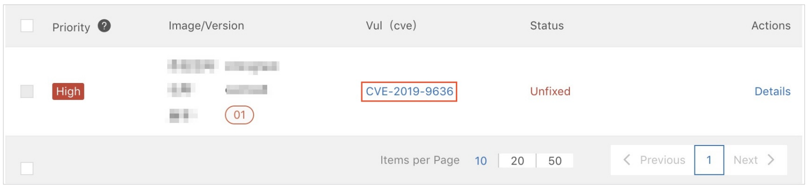
> ? **Note** You can search for vulnerabilities by repository or vulnerability name. Fuzzy match is supported.

- **View vulnerability details**

  Find the vulnerability that you want to view and click **View** in the Operation column. On the page that appears, perform the following operations based on your business requirements:

  - **View the details about the Alibaba Cloud vulnerability library**

    Click the CVE ID to go to the Alibaba Cloud vulnerability library.



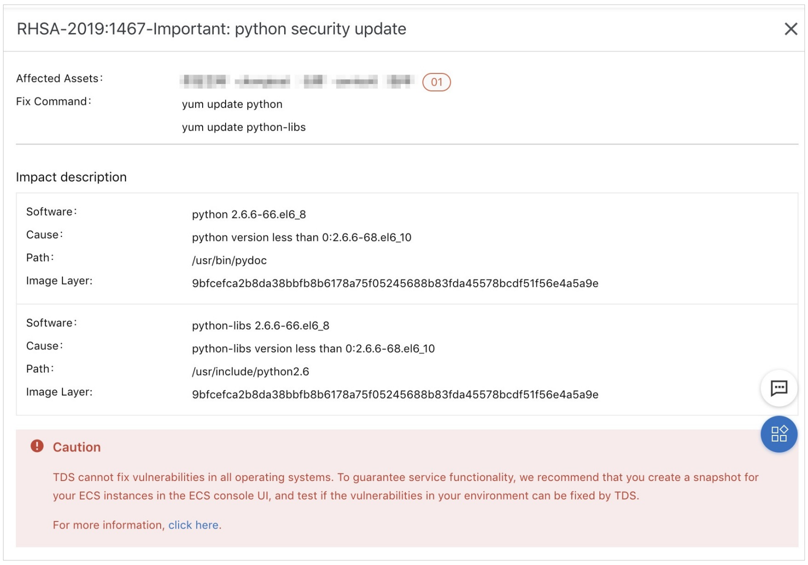
☐	Priority ?	Image/Version	Vul (cve)	Status	Actions
☐	High	[redacted] 01	CVE-2019-9636	Unfixed	Details

☐ Items per Page 10 20 50 < Previous 1 Next >

This library displays detailed information about the vulnerability, including the vulnerability description, basic information, and solution.

- **View fixing commands and impact descriptions**

  Click **Details** to view the fixing commands and impact descriptions.



RHSA-2019:1467-Important: python security update

Affected Assets: [redacted] 01

Fix Command: yum update python
yum update python-libs

Impact description

Software: python 2.6.6-66.el6_8
Cause: python version less than 0:2.6.6-68.el6_10
Path: /usr/bin/pydoc
Image Layer: 9bfcefca2b8da38bbfb8b6178a75f05245688b83fda45578bcdf51f56e4a5a9e

Software: python-libs 2.6.6-66.el6_8
Cause: python-libs version less than 0:2.6.6-68.el6_10
Path: /usr/include/python2.6
Image Layer: 9bfcefca2b8da38bbfb8b6178a75f05245688b83fda45578bcdf51f56e4a5a9e

Caution

TDS cannot fix vulnerabilities in all operating systems. To guarantee service functionality, we recommend that you create a snapshot for your ECS instances in the ECS console UI, and test if the vulnerabilities in your environment can be fixed by TDS.

For more information, click here.

  - **Fix Command**: the fixing command.
  - **Impact description**:
    - **Software**: the image version.
    - **Cause**: the reason why the image is exposed to this vulnerability. In most cases, the reason is that the current version is outdated.
    - **Path**: the path of the image on the server.
    - **Image Layer**: the image layer on which the vulnerability is detected.
  - **Caution**: important notes, prevention tips, and references for the vulnerability.

> **Note** Security Center does not support quick fixes of image system vulnerabilities. You can manually locate and fix the vulnerabilities based on the fixing commands and impact descriptions. After you fix an image system vulnerability, click **Scan Now** on the **Image Security** page to update the vulnerability status on the **Image System Vul** tab.

- **Export the list of image system vulnerabilities**

  You can click the ⤓ icon in the upper-right corner of the vulnerability list to export the list of image system vulnerabilities with a few clicks.

View image application vulnerabilities

1.
2.
3. On the **Image Security** page, click the **Image Application Vul** tab.
4. On the **Image Application Vul** tab, view the detected image application vulnerabilities.

   You can perform the following operations:

   - **View vulnerability announcements**

You can view vulnerability names, vulnerability characteristics, number of affected images, and last scan time.

- **View vulnerability priorities**
  The priorities of vulnerabilities are displayed in different colors in the Affected Assets column. The number in each row of the column indicates the total number of the assets affected by a vulnerability. The following list describes the relationship between colors and priorities:
  - Red: **High**
  - Orange: **Medium**
  - Gray: **Low**

  > **Note** We recommend that you fix the vulnerabilities that have the **High** priority at the earliest opportunity.

- **Filter vulnerabilities**
  On the **Image Application Vul** tab, filter vulnerabilities by vulnerability priority, instance ID, repository name, namespace, digest, or vulnerability name. A vulnerability priority can be high, medium, or low.

  > **Note** You can search for vulnerabilities by repository or vulnerability name. Fuzzy match is supported.

- **View vulnerability details**
  Find the vulnerability that you want to view and click View in the Operation column. On the page that appears, perform the following operations based on your business requirements:
  - **View the details about the Alibaba Cloud vulnerability library**
    Click the CVE ID to go to the Alibaba Cloud vulnerability library.
    This library displays detailed information about the vulnerability, including the vulnerability description, basic information, and solution.
  - **View the fixing commands and impact descriptions**
    Click **Details** to view the fixing commands and impact descriptions.
    - **Fix Command**: the fixing command.
    - **Impact description**:
      - **Software**: the image version.
      - **Cause**: the reason why the image is exposed to this vulnerability. In most cases, the reason is that the current version is outdated.
      - **Path**: the path of the image on the server.
      - **Image Layer**: the image layer on which the vulnerability is detected.
    - **Caution**: important notes, prevention tips, and references for the vulnerability.

- **Export the list of image application vulnerabilities**
  You can click the ⤓ icon in the upper-right corner of the vulnerability list to export the list of image application vulnerabilities with a few clicks.

View the results of image baseline checks

1.

2.
3. On the **Image Security** page, click the **Image Baseline Check** tab.
4. On the **Image Baseline Check** tab, view the results of image baseline checks.

   You can perform the following operations:

   - **Filter the results of image baseline checks**
     You can use the filter above the results of image baseline checks to search for results by severity. The severity can be **Important**, **Medium risk**, or **Low**. You can also enter search conditions in the search box above the results of image baseline checks to search for results by baseline name or type.
   - **View the results of image baseline checks**
     In the results of image baseline checks, you can view the information such as **Baseline Name/Category**, **Affected Mirrors**, **Latest scan time**, **First Scan Time**, and **Status**.
   - **View the details about the result of an image baseline check**
     In the results of image baseline checks, you can find a baseline and click **Details** in the **Operation** column to view the details about the result. You can view information such as the addresses and versions of the images that are affected by the baseline, and the number of baseline risks detected on the images. You can find an image and click **Details** in the **Operation** column. In the **At-Risk Items** panel, you can view the details about the risk items of the image.
   - **Export the results of image baseline checks**

     You can click the ⤓ icon in the upper-right corner of the results of image baseline checks to export the results with a few clicks.

View malicious image samples

1.
2.
3. On the **Image Security** page, click the **Image Malicious Sample** tab.
4. On the **Image Malicious Sample** tab, view the detected malicious image samples.

   > **Notice** A malicious image sample may change the memory attributes from readable and writable to readable and executable or modify the network proxy settings to intrude into your server. We recommend that you handle the malicious image samples at the earliest opportunity.

   You can perform the following operations:

   - **Filter malicious image samples**
     In the upper-left corner of the list of malicious image samples, select **Urgent**, **Suspicious**, or **Notice** to query malicious image samples. You can also filter malicious image samples by instance ID, repository name, namespace, digest, or malicious sample name.
   - **View malicious image samples**
     In the list of malicious image samples, you can view the sample names, number of affected images, first scan time, last scan time, and processing status.
   - **View the details about a malicious image sample**
     Find the malicious image sample whose details you want to view and click **Details** in the **Operation** column.

- **Export the list of malicious image samples**

  You can click the ⤓ icon in the upper-right corner of the sample list to export the list of malicious image samples with a few clicks.

5.FAQ

This topic provides answers to some frequently asked questions about Security Center features. The features include vulnerability fixing, baseline check, and configuration assessment.

- FAQ about Linux software vulnerabilities
  - How do I manually detect Linux software vulnerabilities on my servers?
  - How do I view the current software version and vulnerability details?
  - How do I update kernel 3.1* to kernel 4.4 on Ubuntu 14.04?
  - Do I need to restart my server after I fix a vulnerability?
  - What do I do if Security Center continues to send a vulnerability alert to me after I update the kernel?
  - What do I do If no update is released for the software package that has a vulnerability?
  - How do I view the parameters of Linux software vulnerabilities?
- FAQ about vulnerability fixes
  - How do I fix vulnerabilities?
  - I want to fix multiple vulnerabilities at a time in the Security Center console. What is the fixing order?
  - I fail to create a snapshot when I fix a vulnerability. Why? What do I do?
  - Why does Security Center continue to send alerts to me after I fix vulnerabilities? What do I do?
  - What do I do if the "An error occurred while obtaining the permission. Check the permission and try again." message appears when I fix a vulnerability?
  - Why are the records of the detected vulnerabilities still displayed in the Security Center console after the Security Center agent is disabled or disconnected from Alibaba Cloud?
  - How do I delete a Windows patch from the directory of the Security Center agent?
  - Can Security Center detect Elasticsearch vulnerabilities?
  - How do I handle a connection timeout between my server and the YUM repository of Alibaba Cloud?
  - The "Invalid token" error message appears when I fix a vulnerability. What do I do?
  - What do I do if Security Center fails to verify the fix of a system vulnerability?
  - Can Security Center automatically verify the fix of a vulnerability that requires a system restart?
  - Why does the state of a vulnerability remain unchanged when I verify the vulnerability fix?
  - Why does Security Center fail to roll back a fix for a vulnerability?
- FAQ about vulnerability scans
  - What do I do if I cannot enable the vulnerability detection feature for a server on the Assets page?
  - Are my workloads affected when Security Center scans for urgent vulnerabilities?
  - Why are the results different when Security Center scans multiple times for fastjson urgent vulnerabilities?
  - How often does Security Center detect vulnerabilities?
  - Can Security Center detect system- and application-layer vulnerabilities?
- FAQ about baseline checks
  - What do I do if Security Center fails to verify a fixed baseline check risk?

- What are the differences between baselines and vulnerabilities?

How do I manually detect Linux software vulnerabilities on my servers?

You can use command lines to manually detect Linux software vulnerabilities on your servers. For more information, see How do I manually detect Linux software vulnerabilities?

We recommend that you use the feature provided by Security Center to detect Linux software vulnerabilities. This feature automatically detects vulnerabilities in a timely manner on a regular basis.

How do I view the current software version and vulnerability details?

Security Center compares the software version on your server with the software version that has Common Vulnerabilities and Exposures (CVE) to determine whether your server contains software vulnerabilities. To view vulnerability details of the current software version, you can use one of the following methods:

- **View the current software version and vulnerability details in the Security Center console**
  Log on to the . In the left-side navigation pane, choose **Precaution > Vulnerabilities**. On the Vulnerabilities page, you can view the system software version and vulnerability details. For more information about Linux software vulnerabilities, see How do I view the parameters of Linux software vulnerabilities?.
- **View details of the current software version on your server**
  You can run a command to view details of the current software version:
  - **CentOS**
    Run the `rpm -qa | grep xxx` command. `xxx` specifies the name of the software package. For example, you can run the `rpm -qa | grep bind-libs` command to view the version details of the `bind-libs` software package.
  - **Ubuntu and Debian**
    Run the `dpkg-query -W -f '${Package} -- ${Source}\n' | grep xxx` command. `xxx` specifies the name of the software package. For example, you can run the `dpkg-query -W | grep bind-libs` command to view the version details of the `bind-libs` software package.

    > Note If the specified software package is not found, run the `dpkg-query -W` command to view all the software that is installed on your server.

  After you obtain the version details of the software, compare the version details with the details of the Linux software vulnerabilities detected by Security Center. In the details of a vulnerability, **Software** and **Cause** indicate the version of the current software and the reason based on which Security Center determines that your server has the vulnerability.

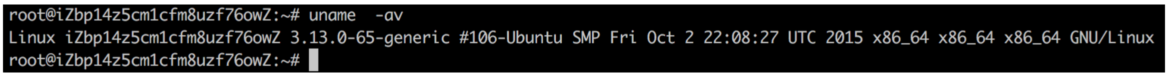
  > Note After you update a piece of software, Security Center may collect the remaining files of the old software version and generate a vulnerability alert on the remaining files. In this case, we recommend that you ignore this alert. Also, you can run the `yum remove` or `apt-get remove` command to delete the software package of the old version. Before you delete the package, make sure that the old software version is no longer required by your workloads or applications.

How do I update kernel 3.1* to kernel 4.4 on Ubuntu 14.04?

> **Notice** Risks may arise when you update the kernel version. We recommend that you follow the instructions provided in Fix software vulnerabilities.

To update kernel 3.1* to kernel 4.4 on Ubuntu 14.04, perform the following steps:

1. Run the `uname -av` command to confirm that the kernel version is 3.1*.



```
root@iZbp14z5cm1cfm8uzf76owZ:~# uname  -av
Linux iZbp14z5cm1cfm8uzf76owZ 3.13.0-65-generic #106-Ubuntu SMP Fri Oct 2 22:08:27 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
root@iZbp14z5cm1cfm8uzf76owZ:~#
```

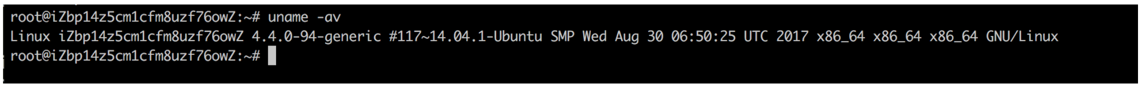
2. Run the following commands to check whether the latest kernel update package is available:

```
apt list | grep linux-image-4.4.0-94-generic
apt list | grep linux-image-extra-4.4.0-94-generic
```

3. If no package is available, run the `apt-get update` command to obtain the latest update package.
4. Run the following commands to install the latest update package:

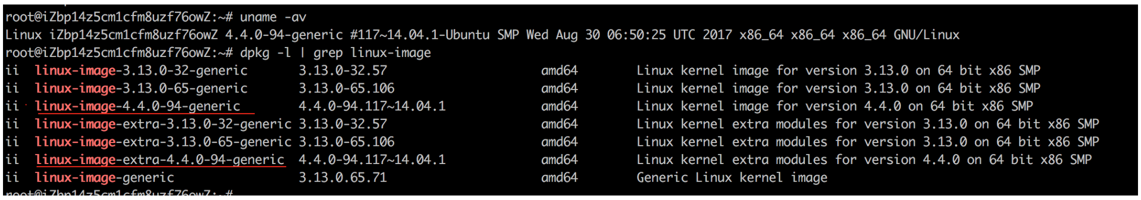
```
apt-get update && apt-get install linux-image-4.4.0-94-generic
apt-get update && apt-get install linux-image-extra-4.4.0-94-generic
```

5. After the update package is installed, restart the server to load the kernel.
6. After the server is restarted, run the following commands to verify the update:
   - Run the `uname -av` command to query the current kernel version.



```
root@iZbp14z5cm1cfm8uzf76owZ:~# uname -av
Linux iZbp14z5cm1cfm8uzf76owZ 4.4.0-94-generic #117~14.04.1-Ubuntu SMP Wed Aug 30 06:50:25 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@iZbp14z5cm1cfm8uzf76owZ:~#
```

   - Run the `dpkg -l | grep linux-image` command to query the details of the current kernel.

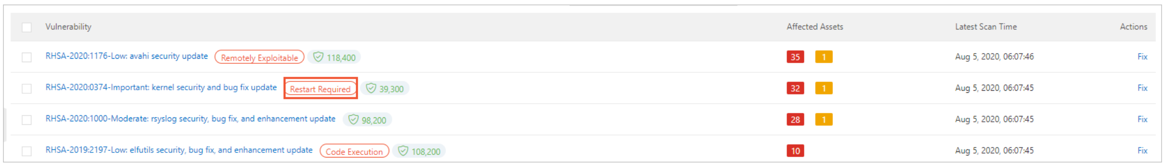


```
root@iZbp14z5cm1cfm8uzf76owZ:~# uname -av
Linux iZbp14z5cm1cfm8uzf76owZ 4.4.0-94-generic #117~14.04.1-Ubuntu SMP Wed Aug 30 06:50:25 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@iZbp14z5cm1cfm8uzf76owZ:~# dpkg -l | grep linux-image
ii  linux-image-3.13.0-32-generic       3.13.0-32.57                amd64        Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-3.13.0-65-generic       3.13.0-65.106               amd64        Linux kernel image for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-4.4.0-94-generic        4.4.0-94.117~14.04.1        amd64        Linux kernel image for version 4.4.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-32-generic 3.13.0-32.57                amd64        Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-3.13.0-65-generic 3.13.0-65.106               amd64        Linux kernel extra modules for version 3.13.0 on 64 bit x86 SMP
ii  linux-image-extra-4.4.0-94-generic  4.4.0-94.117~14.04.1        amd64        Linux kernel extra modules for version 4.4.0 on 64 bit x86 SMP
ii  linux-image-generic                 3.13.0.65.71                amd64        Generic Linux kernel image
root@iZbp14z5cm1cfm8uzf76owZ:~#
```

Do I need to restart my server after I fix a vulnerability?

- Windows servers:
  After you fix a Windows system vulnerability in the Security Center console, you must restart your server to validate the fix.
  This applies to all servers that run Windows.
- Linux servers:
  After you fix a Linux kernel vulnerability in the Security Center console, you must restart your server to validate the fix. This applies if one of the following conditions are met:
  - Your server runs Linux, and the vulnerability that you fix is a Linux kernel vulnerability.

- ○ On the **Linux Software** tab, the vulnerability that you fix is tagged with **Restart Required**. You can perform the following steps to go to the Linux Software tab: Log on to the . In the left-side navigation pane, choose **Precaution** > **Vulnerabilities**.



□	Vulnerability	Affected Assets	Latest Scan Time	Actions
□	RHSA-2020:1176-Low: avahi security update Remotely Exploitable 118,400	35 1	Aug 5, 2020, 06:07:46	Fix
□	RHSA-2020:0374-Important: kernel security and bug fix update Restart Required 39,300	32 1	Aug 5, 2020, 06:07:45	Fix
□	RHSA-2020:1000-Moderate: rsyslog security, bug fix, and enhancement update 98,200	28 1	Aug 5, 2020, 06:07:45	Fix
□	RHSA-2019:2197-Low: elfutils security, bug fix, and enhancement update Code Execution 108,200	10	Aug 5, 2020, 06:07:45	Fix

What do I do if Security Center continues to send a vulnerability alert to me after I update the kernel?

This issue may occur if the remaining files of the old kernel version exist. If you confirm that the alert is triggered due to the remaining files of the old kernel version, you can ignore this alert or delete the remaining files. To fix this issue, you can perform the following steps:

1. After the kernel is updated, run the `uname -av` and `cat /proc/version` commands to view the current kernel version. Make sure that the current kernel version meets the requirement that is described in the vulnerability details.
2. Run the `cat /etc/grub.conf` command to query the configuration file. Make sure that the current system uses the latest kernel version.
3. Security Center determines whether your server contains Linux software vulnerabilities based on the kernel version. If your system contains the Redhat Package Manager (RPM) package of the old kernel version, the package is detected by Security Center, which then generates an alert. Make sure that your system does not contain the RPM package of the old kernel version. If your system contains the RPM package of the old kernel version, delete the package.

> **Note** Before you delete the RPM package of the old kernel version, make sure that the current system uses the latest kernel version. We recommend that you create a snapshot of your system before you delete the RPM package of the old kernel version. If exceptions occur, you can use the snapshot to restore your system.

If you do not want to delete the RPM package of the old kernel version, you can perform the following steps to ignore the alerts that are generated on the old kernel version. Before you ignore the alerts, make sure that the current system uses the latest kernel version.

1. Log on to the Security Center console.
2. In the left-side navigation pane, choose **Precaution** > **Vulnerabilities**.
3. Click the **Linux Software** tab, find the required vulnerability, and then click the vulnerability name. The panel that displays the vulnerability details appears.
4. In the Actions column, click the ⋮ icon and select **Ignore**.

What do I do If no update is released for the software package that has a vulnerability?

Perform the following operations based on your business requirements:

- You may receive one of the following messages when you update software to fix a vulnerability:

```
Package xxx already installed and latest version
Nothing to do
```

or

```
No Packages marked for Update
```

In this case, wait until an official update of the software package is available.
The following software packages do not have available updates:

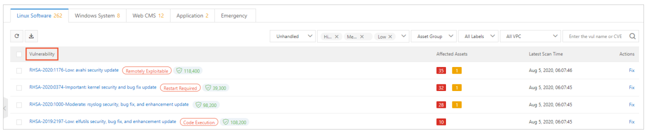
- Gnutls
- Libnl
- MariaDB

- After you update the software package to the latest version, the software package may still fail to meet the version requirement that is described in the Security Center console.
  In this case, check whether the operating system version of your server is supported. For example, since September 1, 2017, CentOS 6.2 to 6.6 and CentOS 7.1 are no longer supported. If your operating system version is not supported, we recommend that you ignore the vulnerability in the Security Center console or update the operating system of your server. If you ignore the vulnerability, the risk may still exist.

How do I view the parameters of Linux software vulnerabilities?

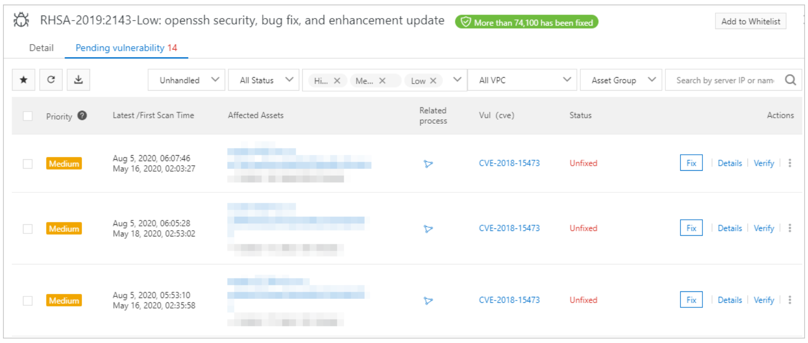
You can log on to the , choose **Precaution > Vulnerabilities**, and then click the **Linux Software** tab to view Linux software vulnerabilities that are detected on your assets. You can click the name of a specific vulnerability to go to the details page. The following list describes the parameters of Linux software vulnerabilities:

- **Vulnerability**
  The notice name of a Linux software vulnerability. The name starts with CVE, RHSA, or USN. Example: RHSA-2016:2972: vim security update.



Vulnerability	Affected Assets	Latest Scan Time	Actions
RHSA-2020:1176-Low: avahi security update Remotely Exploitable 118,400	35 1	Aug 5, 2020, 06:07:46	Fix
RHSA-2020:0374-Important: kernel security and bug fix update Restart Required 39,300	32 1	Aug 5, 2020, 06:07:45	Fix
RHSA-2020:1000-Moderate: rsyslog security, bug fix, and enhancement update 98,200	28 1	Aug 5, 2020, 06:07:45	Fix
RHSA-2019:2197-Low: elfutils security, bug fix, and enhancement update Code Execution 108,200	10	Aug 5, 2020, 06:07:45	Fix

- **Impact**
  The vulnerability impact score, which is based on the open criteria Common Vulnerability Scoring System (CVSS). The score indicates the severity of a vulnerability, which allows you to prioritize the vulnerability.
- **CVE ID**
  The CVE ID of a vulnerability. Example: CVE-2016-XXXX. The CVE system provides a reference method for public information-security vulnerabilities and exposures. You can query the information about vulnerability fixes from all databases that are compatible with CVE to solve security issues.
- **Priority**
  The priority of a vulnerability. Valid values: High, Medium, and Low.



RHSA-2019:2143-Low: openssh security, bug fix, and enhancement update More than 74,100 has been fixed

Priority	Latest /First Scan Time	Affected Assets	Related process	Vul (cve)	Status	Actions
Medium	Aug 5, 2020, 06:07:46 May 16, 2020, 02:03:27	[redacted]		CVE-2018-15473	Unfixed	Fix | Details | Verify
Medium	Aug 5, 2020, 06:05:28 May 18, 2020, 02:53:02	[redacted]		CVE-2018-15473	Unfixed	Fix | Details | Verify
Medium	Aug 5, 2020, 05:53:10 May 16, 2020, 02:35:58	[redacted]		CVE-2018-15473	Unfixed	Fix | Details | Verify

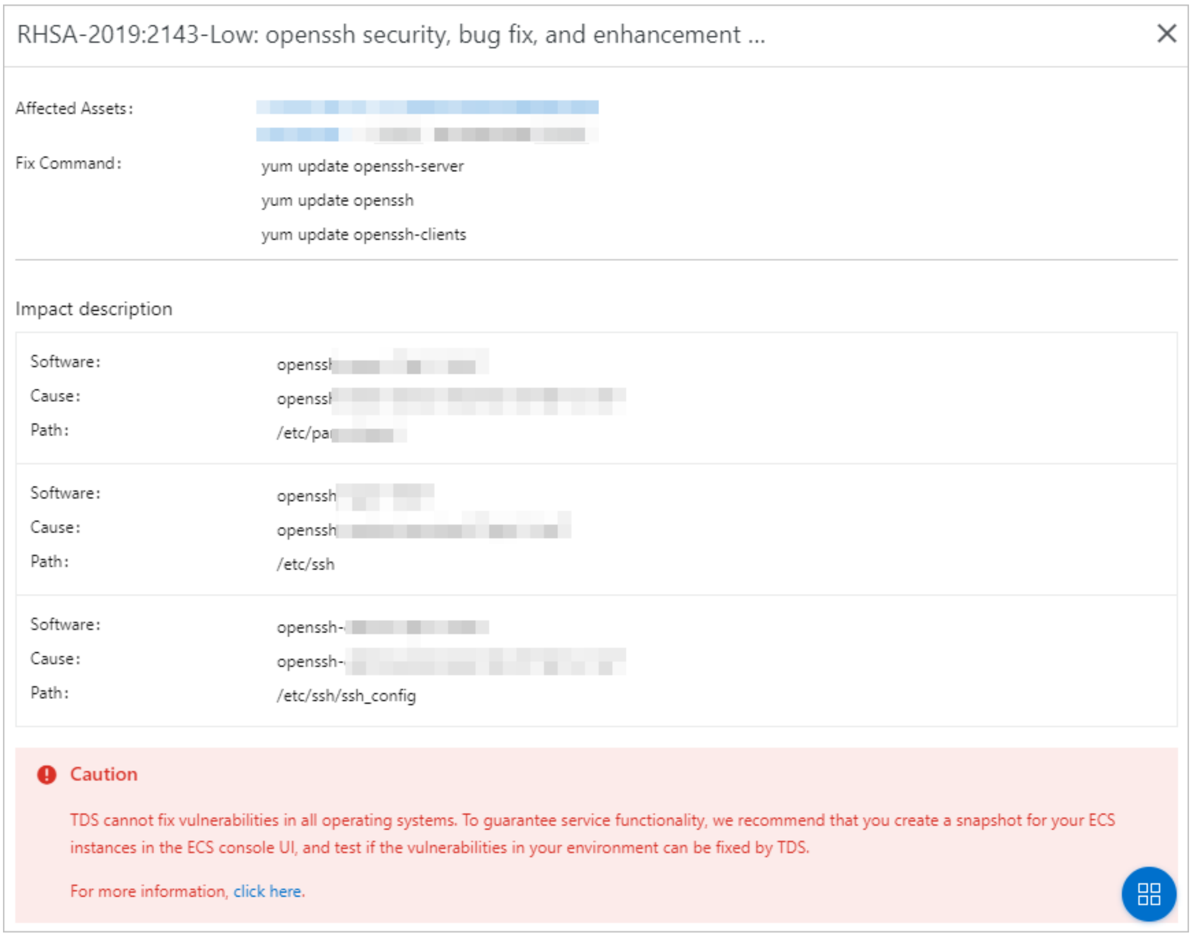
> ? **Note** The vulnerability priority in the preceding figure is **Medium**. You can fix the vulnerabilities based on your business requirements.

- The following vulnerabilities have the **High** priority:
  - Vulnerabilities that attackers can exploit to obtain permissions on the operating system of your server.
  - Vulnerabilities that attackers can exploit to obtain sensitive data and cause data leaks.
  - Vulnerabilities that can cause unauthorized access to sensitive data.
  - Vulnerabilities that can cause large-scale impacts.
- The following vulnerabilities have the **Medium** priority:
  - Vulnerabilities that attackers can exploit to indirectly obtain permissions on the operating system of your server and applications.
  - Vulnerabilities that attackers can exploit to read, write, download, or delete files.
  - Vulnerabilities that can cause sensitive data leaks.
  - Vulnerabilities that can cause workload disruption or remote denial-of-service attacks.
- The following vulnerabilities have the **Low** priority:
  - Vulnerabilities that affect users only during system and user interactions.
  - Vulnerabilities that attackers can exploit to perform unauthorized operations.
  - Vulnerabilities that attackers can exploit after the attackers change the configurations of on-premises machines or obtain important information.
  - Vulnerabilities that can cause on-premises denial-of-service attacks.
  - Vulnerabilities that have minor impacts.

- **Impact description**

  The information about the current version of the software, the reason based on which the vulnerability is detected, and the path of the vulnerability program on your server.

In the panel that displays the details of a vulnerability, you can click **Details** in the Actions column to view the impact description of the vulnerability.



RHSA-2019:2143-Low: openssh security, bug fix, and enhancement ...

Affected Assets: [redacted]

Fix Command:

```
yum update openssh-server
yum update openssh
yum update openssh-clients
```

Impact description

Software: openss[redacted]
Cause: openss[redacted]
Path: /etc/pa[redacted]

Software: openssh[redacted]
Cause: openssh[redacted]
Path: /etc/ssh

Software: openssh-[redacted]
Cause: openssh-[redacted]
Path: /etc/ssh/ssh_config

Caution

TDS cannot fix vulnerabilities in all operating systems. To guarantee service functionality, we recommend that you create a snapshot for your ECS instances in the ECS console UI, and test if the vulnerabilities in your environment can be fixed by TDS.

For more information, click here.

The impact description includes the following items:

- **Software**: the current version of the software. In the preceding figure, the version of mariadb-libs is 5.5.52-1.el7.
- **Cause**: the reason based on which the vulnerability is detected. In most scenarios, the reason is that the software is outdated. In the preceding figure, the vulnerability is detected because the version of mariadb-libs is earlier than 1:5.5.56-2.el7.
- **Path**: the path of the vulnerability program on your server. In the preceding figure, the path of mariadb-libs is */etc/ld.so.conf.d/mariadb-x86_64.con*.

- Actions

  You can perform the following operations on a detected Linux software vulnerability:

  - Fix: Fix the vulnerability.
  - Verify: Check whether the vulnerability is fixed.
  - Ignore: Ignore the vulnerability.

  For more information, see View and handle Linux software vulnerabilities.

How do I fix vulnerabilities?

Security Center can detect Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities, and urgent vulnerabilities. However, Security Center can fix only Linux software vulnerabilities, Windows system vulnerabilities, and Web-CMS vulnerabilities.

Log on to the . In the left-side navigation pane, click Vulnerabilities. On the **Vulnerabilities** page, find the Linux software vulnerability, Windows system vulnerability, or Web-CMS vulnerability that you want to fix and click **Fix** in the Actions column. You can create a snapshot before you fix a Linux software vulnerability or Windows system vulnerability. After you fix a vulnerability, the status of the vulnerability that requires a system restart changes to **Handled (To Be Restarted)**. You must restart your server as instructed before you check whether the vulnerability is fixed.

For urgent vulnerabilities and application vulnerabilities, you can manually fix the vulnerabilities based on the fix suggestions that are provided in the vulnerability details panel. After you fix a vulnerability, you can check whether the vulnerability is fixed on the Vulnerabilities page.

I want to fix multiple vulnerabilities at a time in the Security Center console. What is the fixing order?

Linux software vulnerabilities and Web-CMS vulnerabilities are fixed based on the order of vulnerabilities on the vulnerability list in the Security Center console. For specific Windows system vulnerabilities, pre-patches are required before Security Center can fix the vulnerabilities. When multiple Windows system vulnerabilities are fixed, vulnerabilities that require pre-patches are fixed before other vulnerabilities. Other vulnerabilities are fixed based on the order of vulnerabilities on the vulnerability list in the Security Center console.

I fail to create a snapshot when I fix a vulnerability. Why? What do I do?

When you fix a vulnerability, you may fail to create a snapshot due to the following reasons:

- A RAM user is used to fix the vulnerability: If the RAM user does not have the permissions to create a snapshot, the Security Center console prompts that you cannot create a snapshot. We recommend that you use an Alibaba Cloud account to create a snapshot. For more information about RAM users, see Overview of RAM users.
- Your server is not deployed on Alibaba Cloud: You can create snapshots to fix vulnerabilities only when your server is deployed on Alibaba Cloud.

Why does Security Center continue to send alerts to me after I fix vulnerabilities? What do I do?

This issue occurs because your server is not restarted and the restart is required after you fix vulnerabilities. The vulnerabilities refer to Linux kernel vulnerabilities in this situation. To restart your server, go to the panel that displays vulnerability details and click **Restart** in the Actions column. After your server is restarted, you can click **Verify** in the Actions column. If the status of the vulnerability changes to Handled, the vulnerability is fixed.

What do I do if the "An error occurred while obtaining the permission. Check the permission and try again." message appears when I fix a vulnerability?

This issue occurs because your account does not have permissions to manage the file required to fix the vulnerability. We recommend that you find the vulnerability that you want to fix in the Security Center console and click the vulnerability name. In the panel that appears, view the details of the vulnerability and check whether the owner of the file is the root user. If the owner is not the root user, you must change the owner to the root user. Then, you can go back to the to fix the vulnerability.

Why are the records of the detected vulnerabilities still displayed in the Security Center console after the Security Center agent is disabled or disconnected from Alibaba Cloud?

The records of detected vulnerabilities are displayed in the Security Center console after the Security Center agent is disabled or disconnected from Alibaba Cloud.

After the Security Center agent is disabled or disconnected from Alibaba Cloud for more than three days, all detected vulnerabilities become invalid. In this case, you cannot perform operations on the vulnerabilities. For example, you cannot fix the vulnerabilities or delete the records of the vulnerabilities.

If you do not renew Security Center within seven days after Security Center expires, your data is released and deleted, and the detected vulnerabilities are no longer displayed.

How do I delete a Windows patch from the directory of the Security Center agent?

If you use the Security Center agent to fix a Windows system vulnerability, the Security Center agent automatically downloads, installs, and deletes the patch. If the Security Center agent does not delete the patch three days after the vulnerability is fixed, perform the following steps to manually delete the patch:

1. Log on to the .
2. In the left-side navigation pane, click **Settings**.
3. Optional. Disable client protection for the Security Center agent.
   If client protection was never enabled, skip this step and go to the next step.
   If client protection is enabled, all process files in the directory of the Security Center agent are protected. In this case, Security Center rejects your requests to delete or download a process file from the directory of the Security Center agent.
4. Log on to your server as an administrator.
5. Find the patch and manually delete the patch.
   The path of the patch is *C:\Program Files (x86)\Alibaba\Aegis\globalcfg\hotfix*.

Can Security Center detect Elasticsearch vulnerabilities?

Yes, Security Center can detect Elasticsearch vulnerabilities.

You can perform the following steps: Log on to the . In the left-side navigation pane, choose **Precaution > Vulnerabilities** and click the **Application** tab. Then, check whether Elasticsearch vulnerabilities exist.

> **Note** Only the and editions of Security Center can detect application vulnerabilities. If you use the , , or edition and want to detect application vulnerabilities, you must upgrade Security Center to the Enterprise edition.

How do I handle a connection timeout between my server and the YUM repository of Alibaba Cloud?

If a connection times out, the following error message appears:

```
[Errno 12] Timeout on http://mirrors.aliyun.com/centos/6/os/x86_64/repodata/repomd.xml: (28
, 'connect() timed out!')
```

Make sure that the DNS settings of your server are correct, and wait a while. If the issue persists, submit a ticket to contact after-sales service.

The "Invalid token" error message appears when I fix a vulnerability. What do I do?

If you receive the **Invalid token** error message in the Security Center console, you can refresh the current page and log on to the console again.

> **Note** You can press Ctrl+F5 to forcibly refresh the current page.

What do I do if Security Center fails to verify the fix of a system vulnerability?

To fix this issue, perform the following steps:

1. Check the version information of the vulnerability.
2. Check whether the system uses the YUM repository of Alibaba Cloud.
3. Check whether the fix is verified after a system update.

   > **Note** You must restart the system after you update the kernel.

4. Check whether the destination version of the software update is earlier than the version recommended by Security Center. A later version is required.

If the issue persists, we recommend that you update the operating system.

Can Security Center automatically verify the fix of a vulnerability that requires a system restart?

No, Security Center cannot automatically verify the fix of a vulnerability that requires a system restart.

If a vulnerability is fixed and a system restart is required to verify the fix, the state of the vulnerability is **Handled (To Be Restarted)**. Security Center scans for vulnerabilities on a daily basis. After you fix vulnerabilities of this type, Security Center no longer detects these vulnerabilities. In this case, Security Center retains the information about these vulnerabilities for three days. Make sure that networks can work as expected and no other factors can affect vulnerability detection. After three days, the vulnerability information is deleted.

Why does the state of a vulnerability remain unchanged when I verify the vulnerability fix?

After you run the command generated by Security Center to fix a Linux software vulnerability, the Linux software is updated. The new software version meets the requirement described on the **Vulnerabilities** page of the Security Center console. However, when you click **Verify** in the panel that displays the details of the vulnerability, the state of the vulnerability does not change to Fixed.

To handle this issue, perform the following steps:

- Check the priorities of the vulnerabilities that are detected by Security Center
  Perform the following steps:

  i. Log on to the Security Center console.

  ii. In the left-side navigation pane, choose **Precaution** > **Vulnerabilities**.

  iii. On the **Vulnerabilities** page, click **Settings** in the upper-right corner.

iv. In the **Settings** panel, view **Vul scan level**.

If you do not select a specific priority, Security Center does not automatically update the information about the vulnerabilities that have the priority. You can select priorities based on your business requirements.

- Check whether the version of the Security Center agent is outdated
  If the version of the Security Center agent on your server is outdated, Security Center may not be able to detect vulnerabilities. If the Security Center agent is not automatically updated, we recommend that you manually install the latest version. For more information, see Install the Security Center agent.
- Check whether the Security Center agent is disconnected from Alibaba Cloud
  If the Security Center agent on your server is disconnected from Alibaba Cloud, you cannot verify the fix for the vulnerability. We recommend that you troubleshoot the issue and ensure that the Security Center agent is connected to Alibaba Cloud. For more information, see Identify why the agent is offline.

Why does Security Center fail to roll back a fix for a vulnerability?

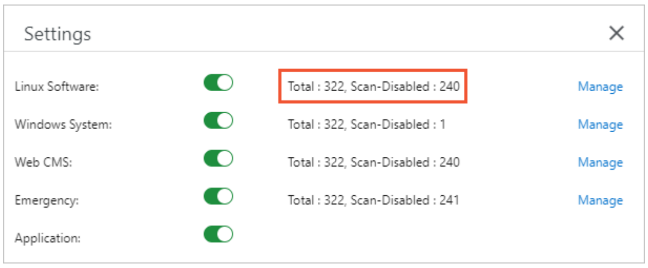
To handle this issue, perform the following steps:

1. Make sure that the Security Center agent on your server is connected to Alibaba Cloud. If the Security Center agent is disconnected from Alibaba Cloud, troubleshoot the issue. For more information, see Identify why the agent is offline.
2. Check whether the files related to this vulnerability are manually modified or deleted.

> **Note** If the related files are manually modified or deleted after the vulnerability is fixed, Security Center cannot roll back the fix.

What do I do if I cannot enable the vulnerability detection feature for a server on the Assets page?

In the upper-right corner of the **Vulnerabilities** page, click **Settings**. In the Settings panel, you can select the servers for which you want to enable the vulnerability detection feature. In the following figure, "Scan-Disabled: 4" indicates that Security Center cannot detect Linux software vulnerabilities for four servers. To enable Security Center to detect Linux software vulnerabilities for the servers, click **Manage**.



Settings

Linux Software:	●	Total : 322, Scan-Disabled : 240	Manage
Windows System:	●	Total : 322, Scan-Disabled : 1	Manage
Web CMS:	●	Total : 322, Scan-Disabled : 240	Manage
Emergency:	●	Total : 322, Scan-Disabled : 241	Manage
Application:	●		

Are my workloads affected when Security Center scans for urgent vulnerabilities?

Security Center checks whether your assets contain urgent vulnerabilities based on the preliminary detection principle. Security Center sends one or two TCP request packets to the IP addresses of all your Elastic Compute Service (ECS) or Server Load Balancer (SLB) instances. The packets do not contain malicious behavior. The feature of urgent vulnerability detection was tested on millions of IP addresses and showed highly stable and reliable performance. However, test environments cannot cover all scenarios. Therefore, unknown risks may still occur. For example, if the business logic of some websites is vulnerable, one or two TCP request packets may cause the server to fail. In this case, your business system may be at risk.

Why are the results different when Security Center scans multiple times for fastjson urgent vulnerabilities?

Whether fastjson vulnerabilities can be detected is based on whether JAR packages are loaded. A web server loads JAR packages in dynamic mode or static mode. In dynamic mode, fastjson vulnerabilities can be detected only if JAR packets are running. Therefore, the scan results are different. We recommend that you scan for fastjson vulnerabilities multiple times to improve the accuracy of scan results.

How often does Security Center detect vulnerabilities?

Security Center can detect vulnerabilities such as Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, urgent vulnerabilities, and application vulnerabilities. You can fix the detected vulnerabilities. The following table lists the default scan cycle and scan mode for vulnerabilities of each type.

Type					
Linux software vulnerabilities	An automatic scan every two days	An automatic scan every day	An automatic scan every day	An automatic scan every day	An automatic scan every day
Windows system vulnerabilities	An automatic scan every two days	An automatic scan every day	An automatic scan every day	An automatic scan every day	An automatic scan every day
Web-CMS vulnerabilities	An automatic scan every two days	An automatic scan every day	An automatic scan every day	An automatic scan every day	An automatic scan every day
Application vulnerabilities	Not supported	Not supported	Not supported	An automatic scan every week. The automatic scan cycle can be modified.	An automatic scan every week. The automatic scan cycle can be modified.
Urgent vulnerabilities	Not supported	Not supported	Not supported. You can specify a scan cycle to perform periodic scans.	Not supported. You can specify a scan cycle to perform periodic scans.	Not supported. You can specify a scan cycle to perform periodic scans.

If you want to enable or disable scans for vulnerabilities of a specific type, or modify the scan cycles for application vulnerabilities and urgent vulnerabilities, click **Settings** in the upper-right corner of the Vulnerabilities page. For more information, see Configure vulnerability settings. If you want to immediately scan for vulnerabilities on your assets, you can use the quick scan feature that is provided by Security Center. For more information, see Use the quick scan feature.

After the vulnerability detection is complete, choose **Precaution** > **Vulnerabilities** in the to view the detection results and handle vulnerabilities if vulnerabilities are detected.

Can Security Center detect system- and application-layer vulnerabilities?

Yes, Security Center can detect system- and application-layer vulnerabilities.

What do I do if Security Center fails to verify a fixed baseline check risk?

To handle this issue, perform the following steps:

- Check whether the version of the Security Center agent is outdated
  If the version of the Security Center agent on your server is outdated, Security Center may fail to verify a fixed baseline risk. If the Security Center agent is not automatically updated, we recommend that you manually install the latest version. For more information, see Install the Security Center agent.
- Check whether the Security Center agent is connected to Alibaba Cloud
  If the Security Center agent on your server is disconnected from Alibaba Cloud, Security Center cannot verify a fixed baseline risk. Make sure that the Security Center agent on your server is connected to Alibaba Cloud. For more information, see Identify why the agent is offline.

What are the differences between baselines and vulnerabilities?

Baselines describe the minimum security requirements for system configurations and management. Baselines include service and application configurations, configurations for operating system components, permission settings, and system management rules. The baseline check feature of Security Center provides security checks for your operating systems, databases, software, and containers. This feature supports the following baseline types: weak passwords, account permissions, identity authentication, password policies, access control, security audit, and intrusion prevention. This way, you can improve system security based on the check results and suggestions provided by Security Center. For more information about check items, see Baselines.

Baseline check is a value-added feature of Security Center. Only users of the , , or edition can use this feature. Users of the or edition must upgrade Security Center to the Advanced or Enterprise edition to use this feature. For more information about upgrades, see Upgrade and downgrade Security Center.