Alibaba Cloud Threat Detection

Precautions

Issue: 20190919

MORE THAN JUST CLOUD | 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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Vulnerabilities

1.1 Vulnerability fix prioritization

The prioritization of vulnerability fixes is essential to cloud asset protection. If you have a large number of assets, Security Center may discover thousands of vulnerabilities on your assets. Such a large number means it is difficult to prioritize the vulnerabilities. To resolve this issue, Security Center provides a set of prioritization standards for you to prioritize these vulnerabilities.

Vulnerability severity score

Security Center uses vulnerability severity scores to prioritize Linux software vulnerabilities and Windows vulnerabilities. Vulnerability fix priorities calculated based on vulnerability severity scores include Urgent, Less urgent, and Not urgent.

> **Note:**
> Emergency vulnerabilities and web content management system (WCMS) vulnerabilities are critical vulnerabilities confirmed by Alibaba Cloud security engineers, which must be fixed immediately.

Vulnerability severity scores can be calculated by using the following formula:

Vulnerability Severity Score = Vulnerability CVSS Base Score x Temporal Score x Environmental Score x Asset Importance Score

The descriptions for these scores are as follows:

- Vulnerability CVSS Base Score: Specifies the CVSS2/3 base score of the vulnerability, in the range of 0 to 10.
- Temporal Score: A temporal score is derived from multiple metrics in the range of 0 to 1. These metrics include the vulnerability exploit maturity and remediation latency.

  In the first three days of the revealing of the vulnerability, the probability of the vulnerability being exploited greatly increases as the public awareness of the vulnerability increases. The temporal score raises from 0 to reach a peak value that is smaller than 1, and then drops quickly. However, as the time passes, the vulnerability becomes more likely to be exploited based on the rapid development

of exploit techniques. The temporal score then gradually increases and approaches 1 within 100 days.

- Environmental Score: Your actual environment is essential to vulnerability prioritization. An environmental score is measured based on your server and the exploitability of the corresponding vulnerability.

  The following environmental factors are currently used to calculate an environmental score:

  - Your server receives traffic from the public network:
    - If the vulnerability can be remotely exploited, the environmental score is 1.5.
    - If the vulnerability can be exploited by attackers in a neighboring network, the environmental score is 1.2.
    - If the vulnerability can be locally exploited, the environmental score is 1.
    - If the vulnerability can only be exploited in a complex environment that cannot be recreated in the cloud, the environmental score greatly decreases.
  - Your server receives traffic only from VPCs:
    - If the vulnerability can be remotely exploited, the environmental score greatly decreases. In this case, the environmental score is set to 0.
    - If the vulnerability can be exploited by attackers in a neighboring network, the environmental score is 1.2.
    - If the vulnerability can be locally exploited, the environmental score is 1.
    - If the vulnerability can only be exploited in a complex environment that cannot be recreated in the cloud, the environmental score greatly decreases.
- Asset Importance Score: Asset importance scores are assigned to servers or assets based on scenarios when large amounts of servers or assets exist.

  Note:
  The default asset importance score is 1.

It takes 48 hours for Security Center to calculate a vulnerability severity score from the time that the vulnerability was detected by Security Center.

Note:

- When a vulnerability is identified, the corresponding authority may have not yet assigned a CVSS base score to the vulnerability. Security Center will provide the

vulnerability severity score 48 hours after the authority has posted the CVSS base score.

- Network malfunctions, such as Security Center agent offline issues, may cause environmental score calculation failures. In this case, the vulnerability severity score is available in 48 hours after your network has recovered.

Vulnerability fix priorities

- Urgent: The recommended vulnerability severity score is in the range of 13.5 to 15.
- Less urgent: The recommended vulnerability severity score is in the range of 7.1 to 13.5.
- Not urgent: The recommended vulnerability severity score is smaller than 7.

Vulnerability fix priorities in special scenarios

- Security Center weights the priority of a vulnerability that has just been detected based on the environment of your server. This process takes 48 hours. During this process, the priority of the vulnerability is measured based on the severity of the vulnerability as follows:
  - If the severity of the vulnerability is critical, the priority is Urgent.
  - If the severity of the vulnerability is high or medium, its priority is Less urgent.
  - If the severity of the vulnerability is low, its priority is Not urgent.
- If the environmental score of a vulnerability cannot be measured due to network convergence, the priority of the vulnerability is set to Not urgent.

1.2 Linux software vulnerabilities

This topic describes how to view and manage Linux software vulnerabilities in Security Center.

Note:
Security Center Basic only supports vulnerability detection. To fix vulnerabilities, you need to activate Security Center Enterprise. For more information about the features provided by Security Center Basic and Enterprise, see #unique_6.

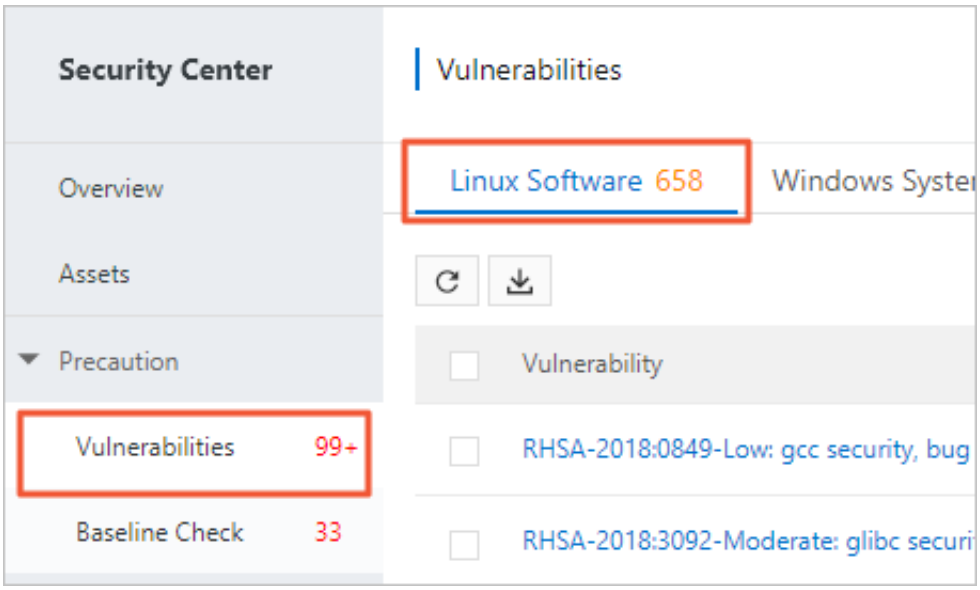
Procedure

1. Log on to the Security Center console.
2. Log on to the Security Center console.

3. Choose Precaution > Vulnerabilities > Linux Software Vulnerabilities.

   On the Linux Software Vulnerabilities page, you can view security bulletins about the Linux vulnerabilities detected by Security Center. Each security bulletin has a title that starts with `USN` , `RHSA` , or `CVE` .

   You can click a security bulletin to view details of the corresponding vulnerabilities.

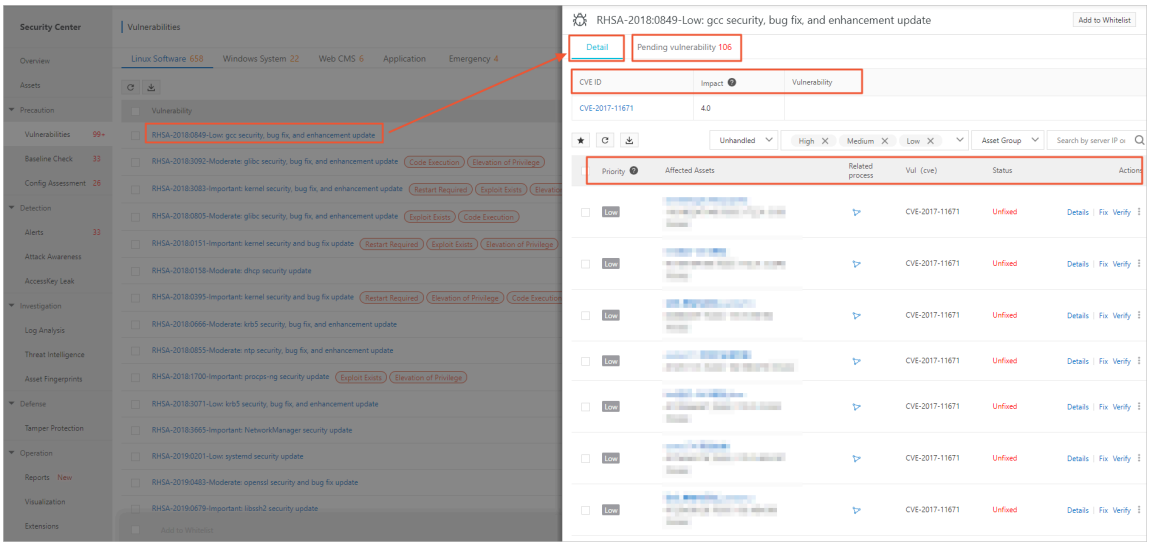


4. On the Linux Software Vulnerabilities page, you can perform the following operations: view security bulletins about the vulnerabilities detected by Security Center, view vulnerability details, fix vulnerabilities, verify whether a vulnerability has been fixed, search vulnerabilities by severity level and status, add vulnerabilities to the whitelist, and ignore vulnerabilities.

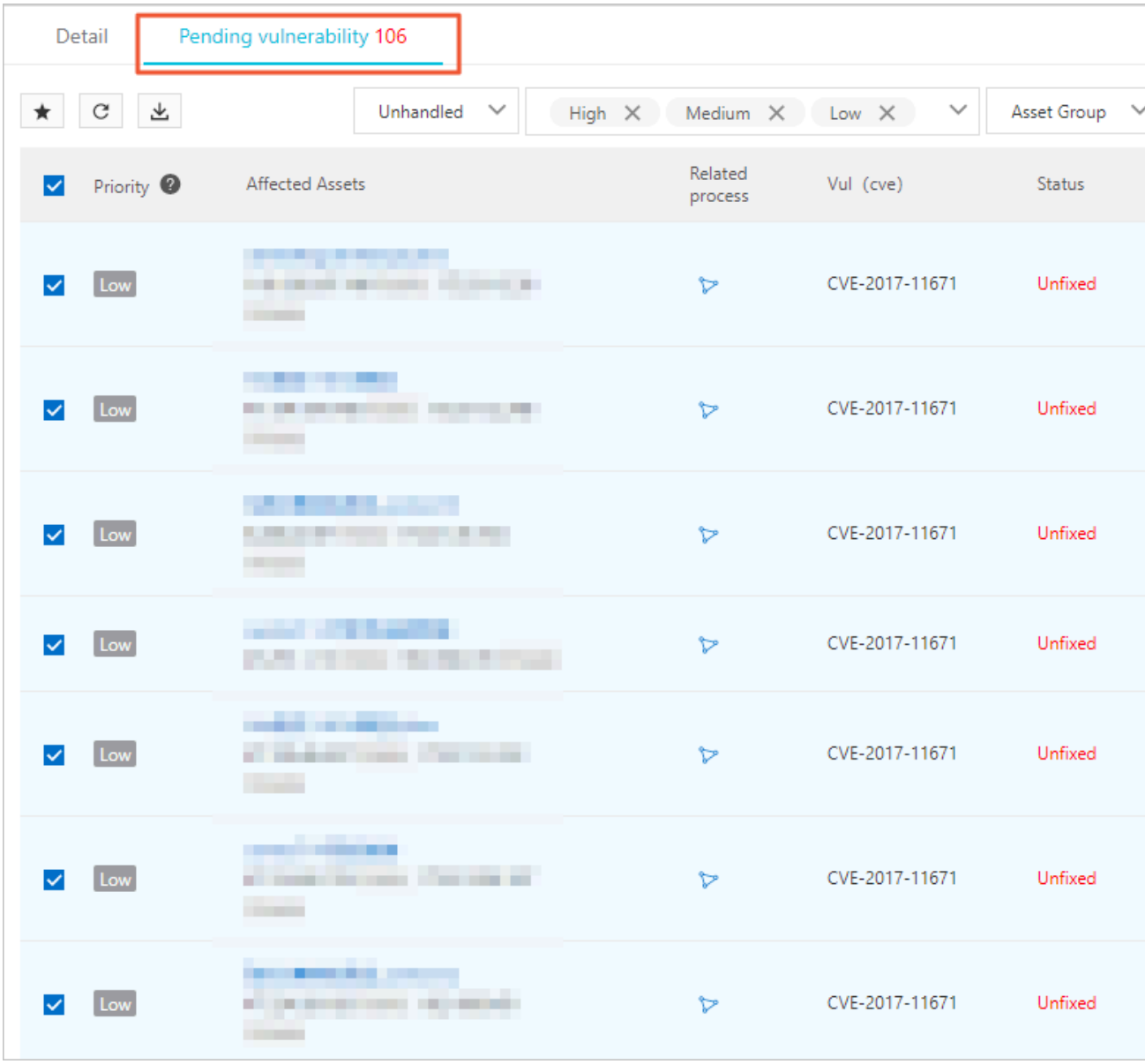
   - View vulnerability details

     Click a vulnerability name to view details. On the vulnerability details page, you can view a description of this vulnerability, its severity level, assets affected by

this vulnerability, and the vulnerability status. You can also choose to fix this vulnerability, verify whether it has been fixed, or ignore it.

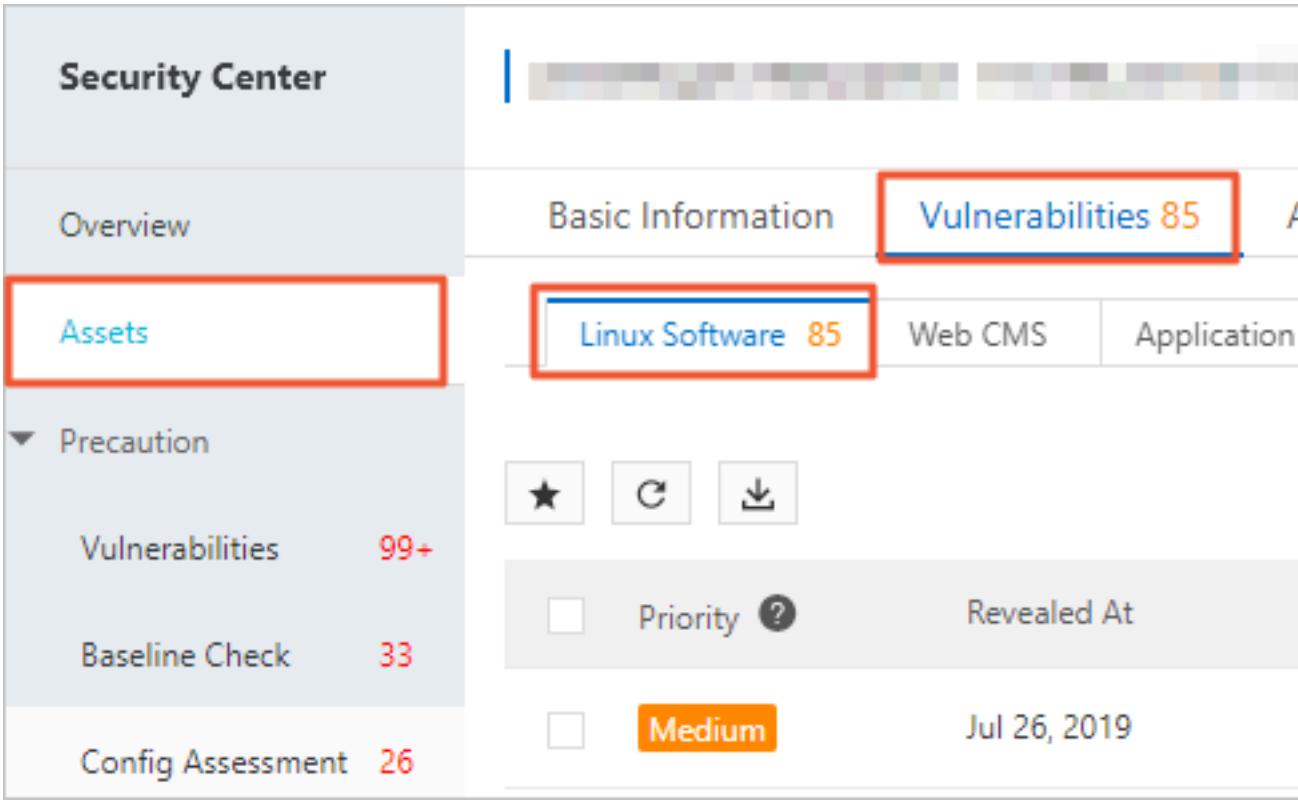


The vulnerability details page also displays information about correlated vulnerabilities and assets that are affected by these vulnerabilities. You can easily analyze and handle these vulnerabilities on this page.



On the vulnerability details page, click an affected asset to view all vulnerabilities that are correlated with the asset. You

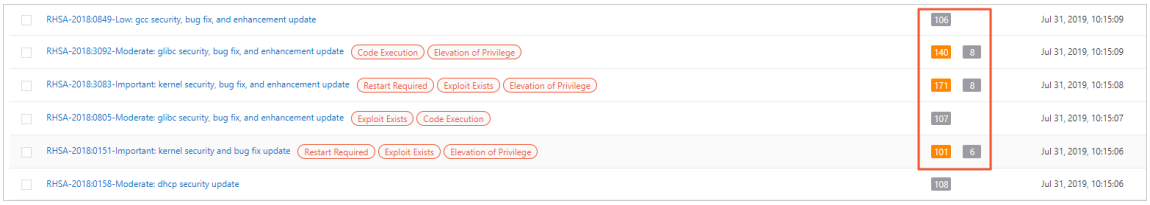
can also choose Assets > Vulnerabilities to open this page.



- Vulnerability priorities (urgency levels)

  Vulnerability priorities are color coded for easy identification.

  - Red indicates high priority.
  - Orange indicates medium priority.
  - Gray indicates low priority.

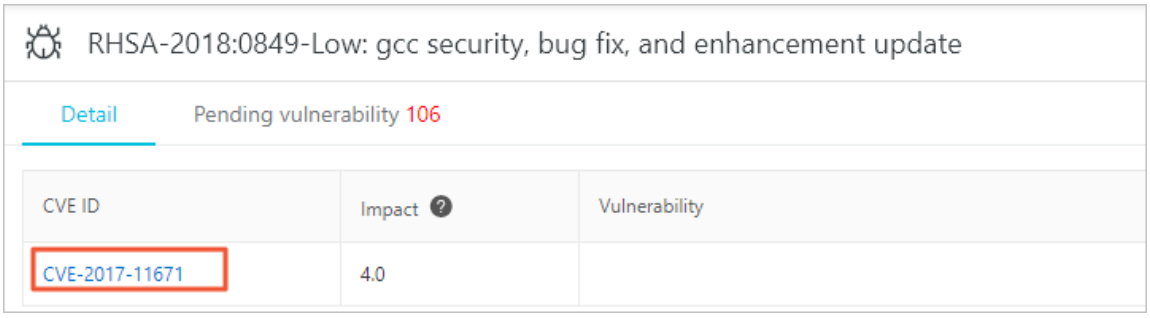


Note:

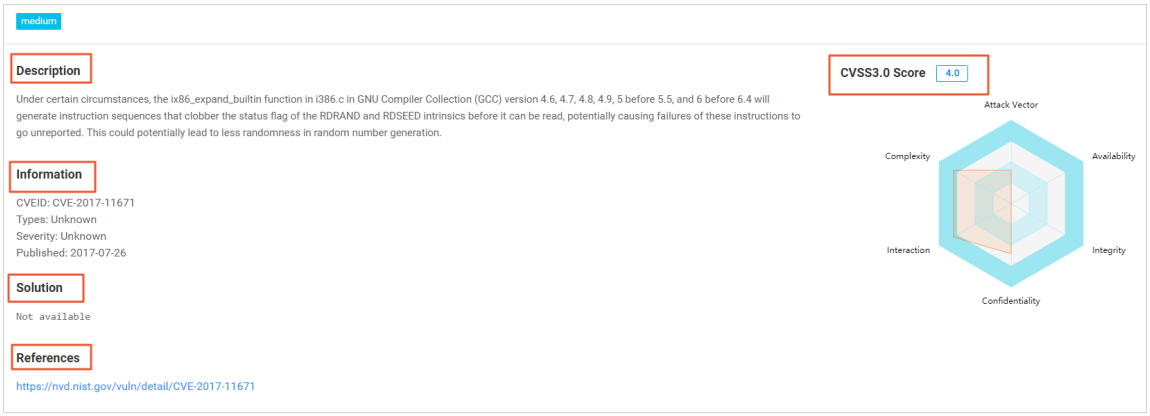
We recommend that you immediately fix high priority vulnerabilities.

- Alibaba Cloud vulnerability library

  On the vulnerability details page, select a vulnerability and click its Vulnerability Number to go to the Alibaba Cloud vulnerability library.



  On the Alibaba Cloud vulnerability library page, you can view more details about this vulnerability, including the detailed description, severity level, time of discovery, and mitigations.



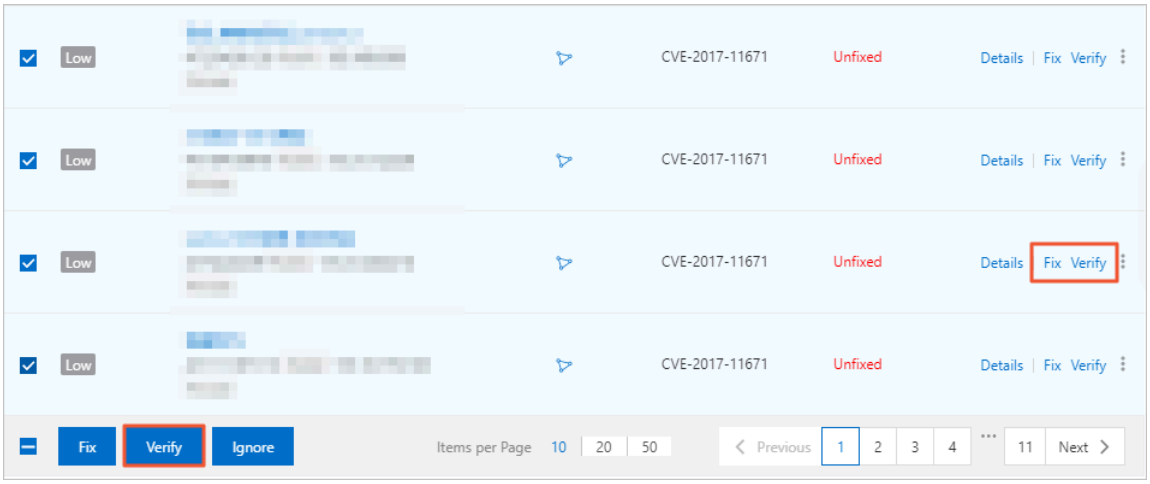
- Vulnerability severity levels (emergency degrees)

  Severity levels are color coded for easy identification. Red indicates important (high severity). Orange indicates moderate (medium severity). Gray indicates low (low severity).

- Verify vulnerabilities

  On the vulnerability details page, you can select one or multiple vulnerabilities and click Verify to verify whether the selected vulnerabilities have been fixed.

  After you click Verify, the vulnerability status is changed to Verifying. It takes several seconds to verify vulnerabilities.



- Fix vulnerabilities

  On the vulnerability details page, you can select one or multiple vulnerabilities and click Fix to fix the selected vulnerabilities.

- Search vulnerabilities

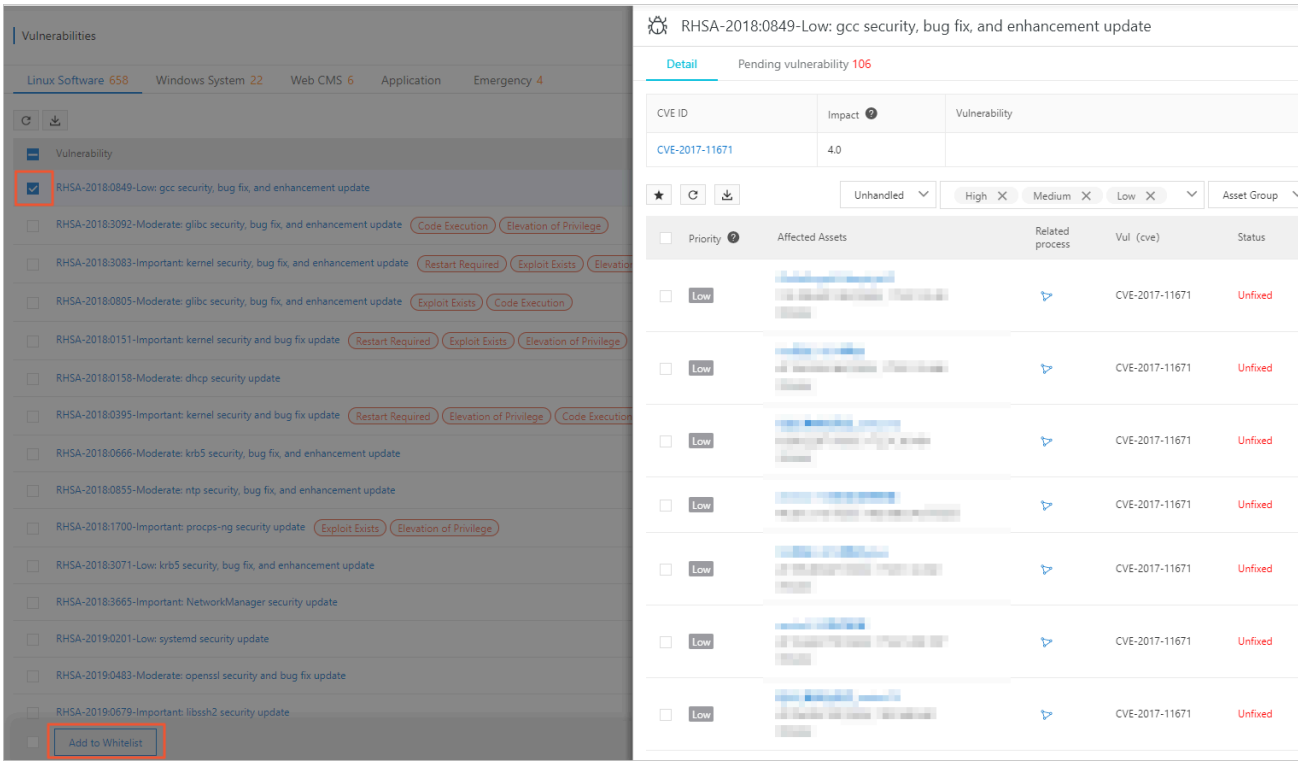
  On the Linux Software Vulnerabilities page, you can search vulnerabilities by vulnerability name, severity level (high, medium, and low), or vulnerability status (handled, unhandled).

Note:
You can also fuzzy search vulnerabilities by name.

- Add vulnerabilities to the whitelist

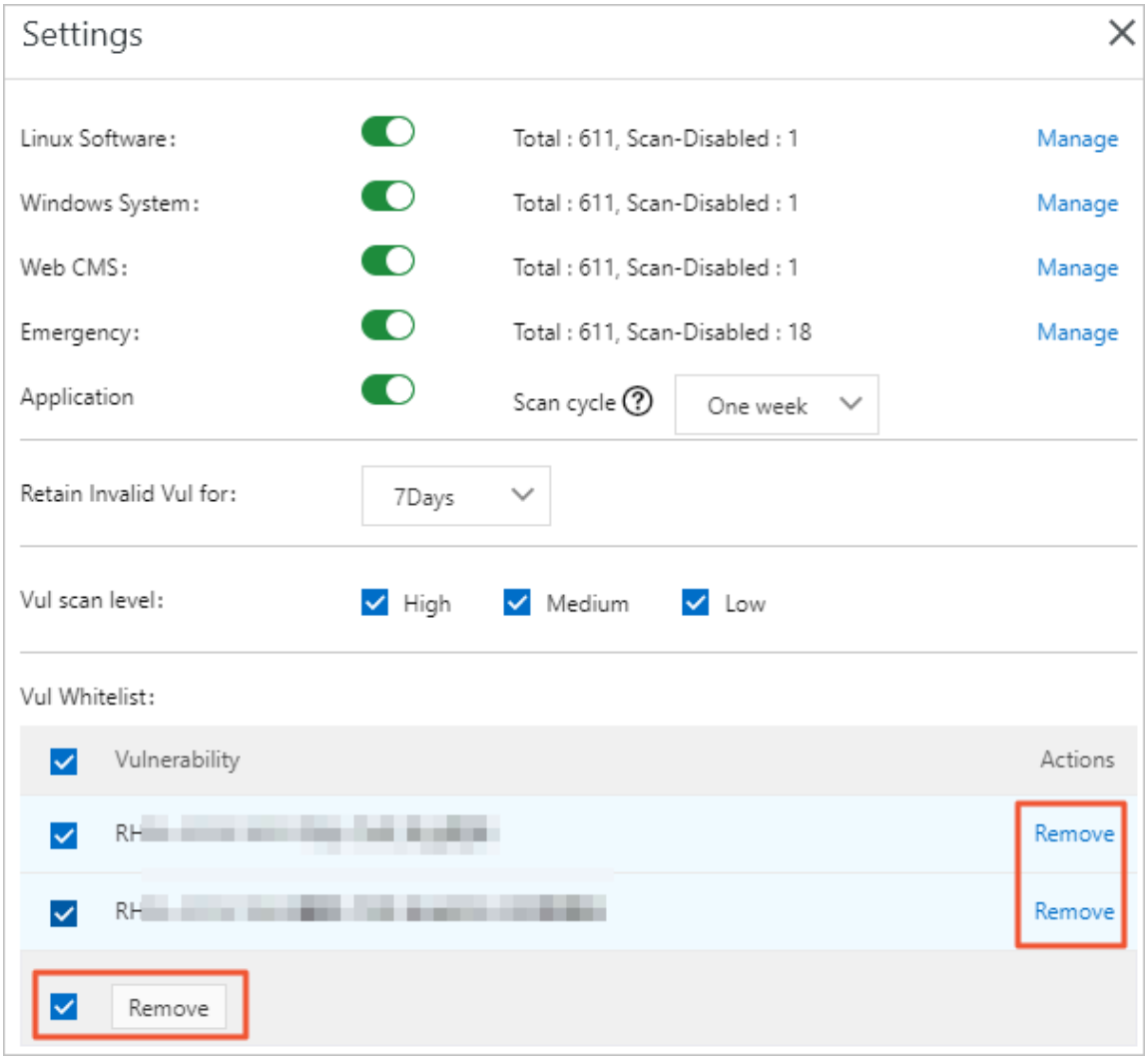
  On the Linux Software Vulnerabilities page, you can select one or multiple vulnerabilities and click Add to Whitelist to add the selected vulnerabilities to

the whitelist. After a vulnerability is added to the whitelist, Security Center does not send alarms when this vulnerability is detected.



Whitelisted vulnerabilities are removed from the vulnerability list on the Linux Software Vulnerabilities page. You can click Settings in the upper-right corner and view these vulnerabilities in the Whitelisted Vulnerabilities table.

If you want Security Center to detect and send alarms on whitelisted vulnerabilities again, select a vulnerability and click Remove to remove this vulnerability from the whitelist on the Settings page.



- Ignore vulnerabilities

  On the Linux Software Vulnerabilities page, you can select one or more vulnerabilities and click Ignore to ignore the selected vulnerabilities.

  > **Note:**
  > After you ignore a vulnerability, the vulnerability status is changed to Handled. If you want Security Center to notify you of this vulnerability again, select this vulnerability in the Handled vulnerability list and click Unignore.

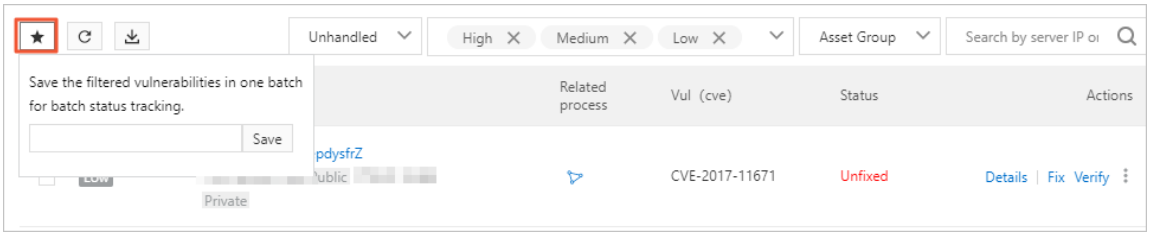
- Export vulnerabilities

  On the Linux Software Vulnerabilities page, you can click the Export icon to export records of all vulnerabilities to your local computer. The exported file is in Excel format.

  > **Note:**

It may take a few minutes to export the records of vulnerabilities depending on the data size.

- On the vulnerability details page, you can click  to save multiple vulnerabilities to a group. This allows you to track vulnerabilities by group.



Vulnerability details

Item	Description
Vulnerability number	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability. The Common Vulnerabilities and Exposures (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 quickly search for information about vulnerability fixes in any CVE-compatible databases to resolve security issues.

Item	Description
Severity score (CVSS score)	The CVSS score follows the widely accepted industry standard, Common Vulnerability Scoring System, and is calculated based on multiple attributes of the vulnerability. This score is used to quantify the severity of vulnerabilities. In the CVSS v3.0 rating system, the severity level indicated by each score is as follows: · 0.0: None. · 0.1-3.9: Low - Vulnerabilities that can cause denial of service. - Vulnerabilities that have minor impacts. · 4.0-6.9: Medium - Vulnerabilities that can impact users during system and user interactions. - Vulnerabilities that can be exploited to perform unauthorized activities. - Vulnerabilities that can be exploited after attackers change local configurations or obtain important information. · 7.0-8.9: High - Vulnerabilities that can be exploited to indirectly obtain user permissions to your server and application systems. - Vulnerabilities that can be exploited to read, download, write , or delete arbitrary files. - Vulnerabilities that can cause sensitive data leaks. - Vulnerabilities that can cause business disruption or remote denial of service. · 9.0-10.0: Critical - Vulnerabilities that can be exploited to directly obtain permissions to the operating system of your server. - Vulnerabilities that can be exploited to directly obtain sensitive data and cause data leaks. - Vulnerabilities that can cause unauthorized access to sensitive information. - Vulnerabilities that can cause large-scale impacts.

Item	Description
Vulnerability name	The name of the vulnerability, which typically starts with CVE. For example, `CVE - 2018 - 1123 on Ubuntu 14 . 04 LTS ( trustly ).`
Affected assets	The server assets that are exposed to this vulnerability, including the servers' public and internal IP addresses.
Priority (Urgency level)	The priority of the vulnerability, including · High: We recommend that you fix high priority vulnerabilities as soon as possible. · Medium: You can fix medium priority vulnerabilities based on your business needs. · Low: You may fix low priority vulnerabilities based on your needs. For more information about fixing vulnerabilities, see #unique_8.
Details	You can select a vulnerability and click Details under the Actions column to view details of this vulnerability. · Commands: The commands you can use to fix this vulnerability. · Impact description: - Software: Version information about the software in the current server. - Cause: The reason why the software is exposed to this vulnerability. Typically, the reason is that the current version is outdated. - Path: The path of the software on the server. · Caution: Important notes, prevention tips, and links to reference documents about this vulnerability.

1.3 Windows software vulnerabilities

Security Center can detect and fix Windows software vulnerabilities.

Synchronized with the security updates released on Microsoft's official website , Security Center can effectively detect important vulnerabilities and notify you

of potential threats. This prevents attackers from exploiting Windows software vulnerabilities to compromise the security of your server.

> Note:
> Security Center Basic only supports vulnerability detection. To fix vulnerabilities, you need to activate Security Center Enterprise. For more information about the features provided by Security Center Basic and Enterprise, see #unique_6.

Procedure

1. Log on to the Security Center console.
2. Log on to the Security Center console.
3. Choose Vulnerabilities > Windows Software Vulnerabilities.

4. On the Windows Software Vulnerabilities page, view security bulletins about the vulnerabilities detected by Security Center, view vulnerability details, fix vulnerabilities, verify whether a vulnerability is fixed, search vulnerabilities by severity level and status, add vulnerabilities to the whitelist, and ignore vulnerabilities.

   - View vulnerability details

     Click a vulnerability name to view details. On the vulnerability details page, you can view a description of the vulnerability, its severity level, assets affected by

this vulnerability, and the vulnerability status. You can also choose to fix the vulnerability, verify whether it is fixed, or ignore it.

The vulnerability details page also displays information about Pending vulnerability and assets that are affected by these vulnerabilities. You can easily analyze and handle these vulnerabilities.

Vulnerability priorities (urgency levels) are color coded for easy identification. Red indicates high priority. Orange indicates medium priority. Gray indicates low priority.

Note:

We recommend that you immediately fix high priority vulnerabilities.

- Verify vulnerabilities

  On the vulnerability details page, you can select one or multiple vulnerabilities and click Verify to verify whether the selected vulnerabilities are fixed.

  After you click Verify, the vulnerability status is changed to Verifying. It takes several seconds to verify vulnerabilities.

- Fix vulnerabilities

  On the vulnerability details page, you can select one or multiple vulnerabilities and click Fix to fix the selected vulnerabilities.

- Search vulnerabilities

  On the Windows Software Vulnerabilities page, you can search vulnerabilities by vulnerability name, severity level (high, medium, and low), or vulnerability status (handled, unhandled).

   Note:
  You can also fuzzy search vulnerabilities by name.

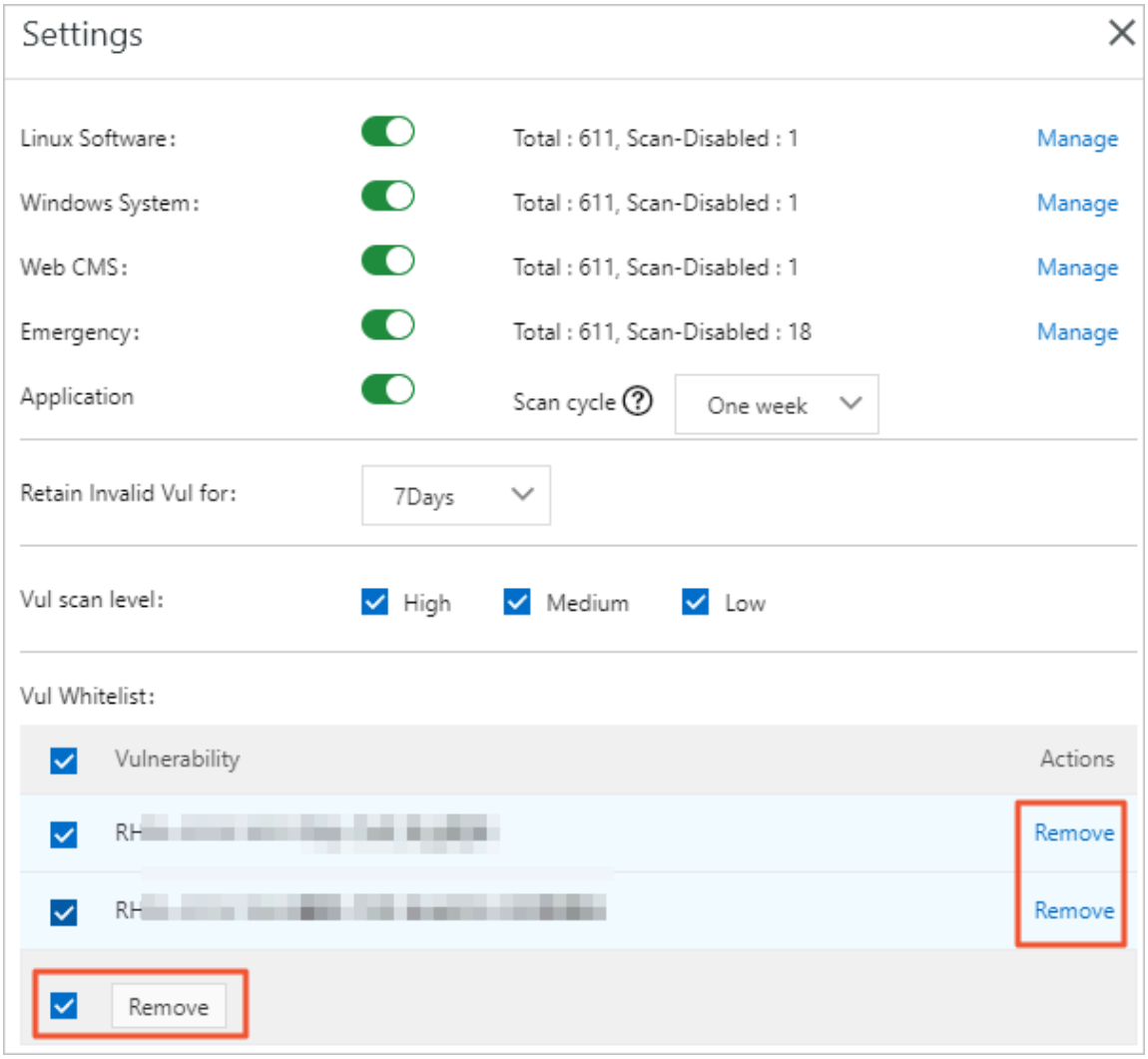
- Add vulnerabilities to the whitelist

  On the Windows Software Vulnerabilities page, you can select one or multiple vulnerabilities and click Add to Whitelist to add the selected vulnerabilities to

the whitelist. After a vulnerability is added to the whitelist, Security Center does not send alarms when this vulnerability is detected.

Whitelisted vulnerabilities are removed from the vulnerability list on the Windows Software Vulnerabilities page. You can click Settings in the upper-right corner and view these vulnerabilities in the Whitelisted Vulnerabilities table.

If you want Security Center to detect and send alarms on whitelisted vulnerabilities again, select a vulnerability and click Remove to remove this vulnerability from the whitelist on the Settings page.



- Ignore vulnerabilities

  On the Windows Software Vulnerabilities page, you can select one or more vulnerabilities and click Ignore to ignore the selected vulnerabilities.

  Note:

After you ignore a vulnerability, the vulnerability status is changed to Handled. If you want Security Center to notify you of this vulnerability again, select this vulnerability in the Handled vulnerability list and click Unignore.

- Export vulnerabilities

  On the Windows Software Vulnerabilities page, you can click the Export icon to export records of all vulnerabilities to your local computer. The exported file is in Excel format.

  Note:
  It may take a few minutes to export vulnerability records depending on the data size.

- On the vulnerability details page, you can click  to save multiple vulnerabilities to a group. This allows you to track vulnerabilities by group.

1.4 Web CMS vulnerabilities

Security Center can detect and fix CMS vulnerabilities. The service can monitor your Web directory, identify common website builders, and detect the vulnerabilities in your system by comparing vulnerable files.

Security Center montiors the latest security vulnerabilities and provides patches and updates in a timely manner. You can download the updates in the console and fix vulnerabilities. The service can help you discover vulnerabilities and provides updates to fix vulnerabilities in batches.

Note:
Security Center Basic only supports vulnerability detection. To fix vulnerabilities, you need to activate Security Center Enterprise. For more information about the features provided by Security Center Basic and Enterprise, see #unique_6.

Note:
Once fixed, CMS vulnerabilities are removed from the console and cannot be detected.

Procedure

1. Log on to the Security Center console.
2. Log on to the Security Center console.
3. Choose Vulnerabilities > Web CMS Vulnerabilities.

4. On the Web CMS Vulnerabilities page, you can perform the following operations: view all CMS vulnerabilities detected by Security Center, fix vulnerabilities, search vulnerabilities by severity level and status, add vulnerabilities to the whitelist, and ignore vulnerabilities.

   - View vulnerability details

     Click a vulnerability name to view details. On the vulnerability details page, you can view a description of this vulnerability, its severity level, assets affected by this vulnerability, and the status of this vulnerability. You can also choose to fix this vulnerability or ignore it.

     The vulnerability details page also displays information about correlated vulnerabilities and assets that are affected by these vulnerabilities. You can easily analyze and handle these vulnerabilities on this page.

     On the vulnerability details page, click an affected asset to view all the vulnerabilities that are correlated with the asset. You can also choose Assets > Vulnerabilities to open this page.

   - Vulnerability priorities (urgency levels)

     CMS vulnerabilities can cause serious damage. Therefore, CMS vulnerabilities have high priority and are marked in red.

     Note:

We recommend that you fix CMS vulnerabilities as soon as possible.

- Search vulnerabilities

  On the Web CMS Vulnerabilities page, you can search vulnerabilities by vulnerability name, severity level (high, medium, and low), or vulnerability status (handled, unhandled).

  Note:
  You can also fuzzy search vulnerabilities by name.

- View vulnerability status
  - Handled
    - Fixed: The vulnerability is already fixed.
    - Fix Failed: An error occurred while fixing the vulnerability. The vulnerable file is already modified or does not exist.
    - Ignored: The vulnerability is ignored. Security Center no longer sends alarms when this vulnerability is detected.
    - Invalid Vulnerability: The vulnerability has not been detected in the last seven days.
    - Fix Undoing Failed: An error occurred while undoing the fix. The vulnerable file may not exist.

    Note:

For handled vulnerabilities, you can choose to undo fixes. When a fix is undone, the vulnerability status is changed to Unhandled.

- Unhandled
  - Unfixed: The vulnerability is yet to be fixed.

- Fix vulnerabilities

  On the vulnerability details page, you can select one or multiple vulnerabilities and click Fix to fix the selected vulnerabilities.

- Ignore vulnerabilities

  On the Web CMS Vulnerabilities page, you can select one or more vulnerabilities and click Ignore to ignore the selected vulnerabilities.

  Note:
  After you ignore a vulnerability, the vulnerability status is changed to Handled. If you want Security Center to notify you of this vulnerability again, select this vulnerability in the Handled vulnerability list and click Unignore.

- Undo fixes

  For handled vulnerabilities, you can choose to undo fixes. When a fix is undone, the vulnerability status is changed to Unhandled.

- Add vulnerabilities to the whitelist

  On the Web CMS Vulnerabilities page, you can select one or multiple vulnerabilities and click Add to Whitelist to add the selected vulnerabilities to

the whitelist. After a vulnerability is added to the whitelist, Security Center does not send alarms when this vulnerability is detected.

Whitelisted vulnerabilities are removed from the vulnerability list. You can click Settings in the upper-right corner and view these vulnerabilities in the Whitelisted Vulnerabilities table.

If you want Security Center to detect and send alarms on whitelisted vulnerabilities again, select the vulnerability and click Remove to remove this vulnerability from the whitelist on the Settings page.

- Export vulnerabilities

  On the Web CMS Vulnerabilities page, you can click the Export icon to export records of all vulnerabilities to your local computer. The exported file is in Excel format.

  > Note:
  > It may take a few minutes to export vulnerability records depending on the data size.

- On the vulnerability details page, you can click  to save multiple vulnerabilities to a group. This allows you to track vulnerabilities by group.

1.5 Emergency vulnerabilities

Security Center can detect and fix emergency vulnerabilities.

The Emergency Vulnerabilities page displays the latest critical vulnerabilities and allows you to check if your assets are affected by these vulnerabilities.

Procedure

1. Log on to the Security Center console.
2. Log on to the Security Center console.
3. Choose Vulnerabilities > Emergency.

4. On the Emergency page, you can view a list of the latest security vulnerabilities and their detailed records.
   - You can click Check Now/Inspect Again on the right side of the Emergency Vulnerabilities page to see if your assets are affected by the selected vulnerability.

Note:

- Currently, Security Center does not show the progress of the check. If threats are detected, you will be notified of the assets with urgent vulnerabilities. You can click an asset name to go to the vulnerability details page and take action.

- If you have a large number of assets, it may take up to 20 minutes to complete the checkup, during which the following message is displayed: No Risk.

· Click a vulnerability name to go to the vulnerability details page. You can find details of this vulnerability, its priority (urgency level), assets affected by this vulnerability, and recommended fixes on this page.

- You can view information about the assets that are affected by this vulnerability.
- You can view the vulnerability status, which can be one of the following:

  ■ Handled

  ■ Fixed: The vulnerability is already fixed.

  ■ Fix Failed: An error occurred while fixing the vulnerability. The vulnerable file is already modified or does not exist.

  ■ Ignored: The vulnerability is ignored. Security Center no longer sends alarms when this vulnerability is detected.

  ■ Invalid Vulnerability: The vulnerability has not been detected in the last seven days.

  ■ Fix Undoing Failed: An error occurred while undoing the fix. The vulnerable file may not exist.

  Note:
  For handled vulnerabilities, you can choose to undo fixes. When a fix is undone, the vulnerability status is changed to Unhandled.

  ■ Unhandled: Unfixed, the vulnerability is yet to be fixed.
- View vulnerability priorities (urgency levels).

  The priority (urgency level) of a vulnerability is determined based on multiple factors, such as the severity of the vulnerability, the time of discovery, and the server's environment.

  Vulnerability priorities (urgency levels) are divided into three types: high, medium, and low.

  Note:

We recommend that you immediately fix high priority vulnerabilities.

- Handle emergency vulnerabilities.

  ■ Verify: You can verify if a vulnerability is already fixed.

  ■ Ignore: You can ignore a vulnerability so that Security Center does not send alarms when this vulnerability is detected.

  Note:
  After you ignore a vulnerability, the vulnerability status is changed to Handled. If you want Security Center to notify you of this vulnerability again, select this vulnerability in the Handled vulnerability list and click Unignore.

1.6 Vulnerability management settings and whitelist configuration

The vulnerability management settings allow you to enable or disable automatic detection for different types of vulnerabilities. It also allows you to enable vulnerability detection on specific servers, set a time period for keeping invalid vulnerabilities, and configure a vulnerability whitelist.

You can select multiple vulnerabilities from the list of Linux software vulnerabilities , Windows system vulnerabilities, and Web-CMS vulnerabilities, and whitelist the selected vulnerabilities. Security Center does not detect a whitelisted vulnerability. You can manage the vulnerability whitelist in the vulnerability management settings.

Procedure

1. Log on to the Security Center console.
2. Choose Precaution > Vulnerabilities > Settings.
3. On the displayed Settings page, you can perform the following operations:

   · Click the toggle on the right of a vulnerability type to enable or disable vulnerability detection.

   · Click Manage to add servers for vulnerability detection.

   · Set the time period for keeping invalid vulnerabilities to 7 days, 30 days, or 90 days.

   Note:

If you do not take any action on a detected vulnerability, the system determines that the alert on this vulnerability is invalid. The system automatically removes this vulnerability after the specified period.

- In Vul Whitelist, select a vulnerability, and click Remove to enable vulnerability detection and alerting.

1.7 Software vulnerability fix

This topic introduces the best practice for fixing software vulnerabilities on servers.

You can use the following method to fix vulnerabilities that have been detected on your server by the vulnerability detection feature of Security Center.

Note:
This method is designed to successfully fix vulnerabilities detected in the operating system, network devices, databases, and middleware on servers.

How to fix software vulnerabilities

Unlike fixing vulnerabilities on PCs, fixing software vulnerabilities on servers requires expert knowledge. You must follow these steps to fix software vulnerabilities :

Prerequisites

1. You must check all assets on the target server and log on to the Security Center console to check system vulnerabilities on the server. For more information about descriptions of Linux software vulnerability attributes in Security Center, see Linux software vulnerability attribute descriptions.
2. After checking the system vulnerabilities on the target server, determine the vulnerabilities that need to be fixed urgently. You can determine which vulnerabil ities need to be fixed urgently based on the business status, server status, and impacts caused by vulnerability fixes.
3. Upload vulnerability patches to the testing environment, test the compatibility and security of these patches, and then generate a vulnerability fix testing report. The vulnerability fix testing report must include vulnerability fix results, vulnerability fix duration, patch compatibility, and impacts caused by vulnerability fixes.
4. To prevent exceptions, before fixing the software vulnerabilities, you must use the backup and recovery feature to back up the system of the target server. For

example, you can use the snapshot feature of ECS to create a snapshot of the target ECS instance.

Fix vulnerabilities

1. Upload the vulnerability patches to the target server and use the patches to fix the vulnerabilities. This task requires a minimum of two administrators: One administrator takes charge of fixing vulnerabilities and the other one takes charge of making records. Exercise all operations with caution.
2. The administrator must follow the system vulnerability list sequentially to upgrade the system and fix vulnerabilities.

Validate vulnerability fixes and generate a report

1. Validate the vulnerability fixes on the target server. Make sure that the vulnerabilities have been successfully fixed and that no exceptions have occurred on the target server.
2. Generate a vulnerability fix report based on the entire vulnerability fix process and archive the relevant documents.

Software vulnerability fix guidelines

To make sure that the operating system of the target server can run normally during the software vulnerability fix process, and to minimize the possibility of exceptions, follow these guidelines when you fix vulnerabilities:

- Create a vulnerability fix plan

  You must inspect the operating system and application system of the target server and create a applicable vulnerability fix plan. The feasibility of the vulnerability fix plan must be discussed and verified in the testing environment. You must strictly follow the instructions and steps in the vulnerability fix plan to fix vulnerabilities and make sure that no damage is made to the systems of the target server.
- Use a testing environment

  You must use a testing environment to verify the feasibility of your vulnerability fix plan. Make sure that the plan has no impacts on the online business system to be fixed.

   Note:

The testing environment must use the same operating system and database system as your online business system. The application system version of the testing environment must be the same as your online business system. We recommend that you use the latest replica of the entire business system for testing.

- Back up your business system

  You must back up the entire business system, including the operating system, applications, and data. After backup, you must validate the backup by restoring your system. System backup guarantees the availability of your business. If a system exception or data loss occurs, you can use the backup to restore your system. We recommend that you use the snapshot feature of ECS to quickly back up your business system.

2 Baseline check

2.1 Baseline Check overview

This topic describes how to use the Baseline Check feature and handle the configurat ion risks on your servers.

Features

After you activate Baseline Check, Security Center automatically detects risks related to the systems, accounts, databases, passwords, and security compliance configurations of your servers, and provides resolutions. For more information on the check items, see Baseline Check items.

Security Center automatically checks your baseline configurations from 00:00 to 06 :00 every day. You can create the check policies and manage the policies. When you create or modify a policy, you can customize the items, the cycle, and the time of a baseline check, and select the servers to which you want to apply this policy.

Restrictions

Baseline Check is a value-added service of Security Center. Only Enterprise Edition or users can activate and use this service. A Basic Edition or Pro Edition user must upgrade to Enterprise Edition to use this service.

Logon attempts may be required to check for weak passwords on applications such as MySQL and SQL Server. This leads to server resource consumption and many logon failure records. Therefore, Security Center disables the check for weak passwords on specific applications and system compliance with classified protection standards by default. To check these items, make sure that you are aware of the risks mentioned above, and select these items when you customize a scan policy.

Baseline Check items

Category	Check item
Database	Risks in the port listening configuration of Redis or Memcached and risks in the configuration of the permission to start Redis or Memcached.

Category	Check item
System	The classified protection standard compliance check covers check items in the level 2 and level 3 security requirements stated in China Classified Protection Standard 2.0. The security baseline check follows the security standards of Alibaba Cloud and Center for Internet Security (CIS). Security Center checks these items on the following systems: · CentOS Linux 6 and Linux 7 · Linux Ubuntu · Debian Linux · Windows 2008 R2 and 2012 R2
Weak password	PostgreSQL weak password
	SSH weak password
	Anonymous FTP logon
	SQL Server weak password
	MySQL weak password
	RDP weak password
	FTP weak password
Middleware	Apache Tomcat security baseline

2.2 Create and configure a baseline check policy

This topic describes how to create, modify, or delete a baseline check policy.

Baseline check is a value-added service of Security Center. Only Enterprise Edition users can activate and use this service. A Basic Edition or Pro Edition user must upgrade to Enterprise Edition to use this service.

After you activate this service, Security Center automatically scans all assets based on the default policy. The details of this check are as follows:

Time: From 06:00 to 12:00 every day.

Object: All assets under your Alibaba Cloud account.

You can also customize a baseline check policy that covers the baseline items that are not covered by the default policy.

Procedure

1. Log on to the Security Center console.
2. In the left-side navigation pane, click Baseline Check.
3. In the upper-right corner, click Manage Policies to customize a policy or modify the default policy.
   - In the upper-right corner of the Manage Policies page, click Create Policy.

Configuration item	Description
Policy Name	Enter a policy name.
Cycle	Set the cycle to 1 day, 3 days, 7 days, or 30 days. Set the time to 00:00-06:00, 06:00-12:00, 12:00-18:00, or 18:00-24:00.
Check Items	Select check items under the categories including database, system, weak password, and middleware baseline. For more information about baseline check items, see Baseline check items.
Servers	Select the asset groups to which you want to apply this policy. Note: New servers belong to Asset Groups > Default by default. To apply this policy to new servers, select Default.

   - On the Manage Policies page, click Edit or Delete to modify or delete a specified policy.

     Note:
     You cannot restore a deleted policy.

   - Click Edit next to the Default policy. You can select the asset groups to which the default policy is applied.

     Note:

You cannot delete the default policy or modify the check items in the default policy.

- Below the Manage Policies page, you can set the level range (high, medium, low) for the baseline check.

2.3 Baseline check

This topic describes how to check the baselines by using customized policies, and how to view the check results and suggestions on handling baseline risks.

Context

Baseline check is a value-added service of Security Center. Only Enterprise Edition users can activate and use this service. A Basic Edition or Pro Edition user must upgrade to Enterprise Edition to use this service.

View the summary data for the check result

In the upper part of the Baseline Risk page, you can view the summary data for the baseline check result.

- Checked Servers: The number of servers on which baseline check is performed.

  Checked Servers indicates the number of servers that you select when configuring a check policy.
- Check Items: The number of check items that you select when configuring a scan policy.
- Last Check Pass Rate: The pass rate of the last baseline check.

  If the number in the Last Check Pass Rate area is green, the pass rate of the checked servers is high. If this number is red, a large number of baseline risks have been detected. We recommend that you view the check result details and deal with the failed items.

Manually perform a baseline check

Both automatic periodical check and manual check are supported. To schedule a periodical check, set Cycle and Time when configuring a scan policy. To manually begin a check, click Check Now.

1. Log on to the Security Center console.
2. In the left-side navigation pane, click Baseline Check.
3. In the Select Policy drop-down list, select a policy for a manual check.

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

4. Click Check Now.

   After you click Check Now, the progress of the check is displayed.

   You can click View Progress to view the number of servers that have passed or failed the check and the causes of the failures. Click View Solution to learn how to handle the failures.

   Click Refresh to view the latest check result.

View detailed check results

After a baseline check is complete, you can click a baseline in the list to enter the details page of this baseline. This page displays the assets affected by this baseline, the failed and passed items of each asset, and the suggestions on risk handling. You can also ignorefailed items or verify fixed risks.

1. Log on to the Security Center console.
2. In the left-side navigation pane, click Baseline Check.
3. In the baseline list, click a baseline.

4. On the details page of the selected baseline, you can:

   - View the information about all assets affected by this baseline.

   - Click View next to an asset to view the at-risk baseline items on this asset and the check result of each item. The check result can be failed or passed.

      Note:
     We recommend that you handle the failed items immediately.

   - If you do not want to receive alerts for risks on an item, select this item and click Ignore to remove it from the alert list. An ignored item no longer triggers alerts.

      Note:
     To ignore multiple items, select the items, and click Ignore below the item list of the asset.

   - Click Details next to an item to view the item description, check result, and suggestions.

     We recommend that you enhance the baseline configurations based on the suggestions.

      Note:
     We recommend that you handle the failed items of high severity immediately.

   - After you handle a failed item, click Verify to check whether the risk has been cleared. After you begin verifying an item, the item status becomes Verifying.

     If you have not verified an item, Security Center automatically verifies this item during the next periodical check.

3 Cloud Platform Configuration Assessment

The Cloud Platform Configuration Assessment feature of Security Center checks the security configuration of your cloud services. The checks are performed from five perspectives, including identity authentication, network access control, data security, log auditing, and basic security configuration. This feature helps you detect configuration risks in your cloud services and provides suggestions on risk handling.

This feature is available only in Security Advanced or Enterprise edition. If you are a Basic Edition user and want to use this feature, upgrade to Advanced or Enterprise Edition.

Procedure

1. Log on to the Security Center console.
2. In the left pane, click Config Assessment.
3. On the Cloud Platform Configuration Assessment page, click Authorize Now. The Cloud Resource Access Authorization page is displayed.
4. Click Confirm Authorization Policy to allow Security Center to access your cloud resources.

   After the authorization, you can use the Cloud Platform Configuration Assessment feature to check for configuration risks on your cloud services and handle these risks.

   This feature supports the following operations:

   - Settings: You can set the days and time frame for configuration checks.

     Select one or multiple days from Monday to Sunday.

     Each day is divided into four time frames. Select one time frame. During the selected time frame on the selected day, Security Center automatically checks all

the check items. By default, TDS automatically checks your configurations from 00:00 to 06:00 once every other day.

- Check Now: Check for risks on all configuration items of your cloud services and identify the number of affected assets. The check items are listed by risk severity, in the order from the highest severity to the lowest severity.

  Security Center can check the following types of items:

  - Cloud platform - primary account two-factor authentication configuration
  - Cloud platform - ActionTrail configuration
  - Alibaba Cloud Security - Anti-DDoS Pro back-to-origin configuration
  - Security group - RDS whitelist configuration
  - SLB - open vulnerable ports
  - Alibaba Cloud Security - WAF back-to-origin configuration
  - OSS sensitive file leaks
  - RDS - database security policies

   Note:
  Wait until the check is complete to perform other operations.
- Verify: Verify whether risks exist on a specific item. If you have modified the configuration of a check item, you can click Verify to check for risks on this item.
- Click the name of a check item to view the details, including the description, risks, and solutions.
- Ignore: If you confirm that an at-risk item is secure, you can click Ignore. This changes the item status to Ignored. An ignored item is not included in at-risk items.

  You can also Unignore an ignored item.

   Note:
  Ignored items are not included in the at-risk items in later checks.
- Label as False Positive: If you confirm that the alert on a check item is a false positive, click Label as False Positive. This changes the item status to Labelled as False Positive.

   Note:

An item that has been labelled as a false positive is not included in the at-risk items in later checks.