

Alibaba Cloud

Cloud Firewall Security Notification

Document Version: 20200922

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.[Virtual patch] Authentication bypass vulnerability in Apache...	06
2.[Virtual patch] Apache Dubbo remote code execution vulner...	07
3.[Virtual patch] Remote code execution vulnerability (CVE-202...	08
4.[Virtual patch] Apache Tomcat AJP file read and inclusion vu...	09
5.[Threat intelligence] Apache Dubbo deserialization vulnerabi...	10
6.[Virtual patch] Remote command execution vulnerability (CVE...	11
7.[Basic rule] Remote code execution vulnerability in e-cology	12
8.[Virtual patch] Remote command execution vulnerability in N...	13
9.[Threat intelligence] Remote code execution vulnerability (CV...	14
10.[Virtual Patches] Remote code execution vulnerability in Re...	15
11.[Virtual Patches] Remote command execution vulnerability i...	16
12.[Virtual Patches] Remote code execution vulnerability (CVE-2...	17
13.[Virtual patch] WebLogic wls9-async deserialization remote ...	18
14.[Threat notice] Unauthorized access to MongoDB	19
15.Confluence remote file reading vulnerability (CVE-2019-3396)	20
16.[Threat Intelligence] Attacks on Jenkins	21
17.[Virtual Patches] Remote code execution vulnerability in Ne...	22
18.[Basic Policies] Remote code execution vulnerability in Jenki...	23
19.[Virtual patch] User privilege escalation vulnerability in Kub...	24
20.[Basic rule] Remote code execution vulnerabilities in multipl...	25
21.[Basic rule] Remote code execution vulnerabilities in ThinkP...	26
22.[Basic rule] Malicious file writing vulnerability of PostgreSQL	27
23.[Threat intelligence] Multiple botnets exploit the ThinkPHP ...	28
24.[Virtual patch] ThinkPHP 5.x remote command execution (g...	29
25.[Basic rule] Update of Bash reverse shell detection rules	30
26.[Basic rule] Update of mining pool communication detectio...	31

27.[Basic rule] PHPCMS 2008 code injection vulnerability (CVE-2...	32
28.[Virtual patch] WebLogic T3 deserialization vulnerability	33
29.[Threat intelligence] Redis unauthorized access vulnerability	34
30.[Basic rule] Remote command execution through Microsoft ...	35
31.[Virtual patch] Nginx security issues cause servers' vulnerab...	36
32.[Threat intelligence] QBotVariant attack	37
33.[Threat intelligence] DDG mining botnet attack	38
34.[Basic rule] Malicious MySQL UDF execution	39
35.[Virtual patch] Arbitrary file upload vulnerability of WebLog...	40
36.[Threat intelligence] REST API unauthorized access vulnerab...	41

1.[Virtual patch] Authentication bypass vulnerability in Apache Shiro versions earlier than 1.6.0 (CVE-2020-13933)

On August 17, 2020, Alibaba Cloud emergency response center detected that Apache Shiro had officially released a security update that fixed the latest authentication bypass vulnerability. Attackers can exploit this vulnerability to access the Shiro server after bypassing the authentication process.

Apache Shiro is a widely used framework for permission management and user authentication and authorization. The authentication bypass vulnerability (CVE-2020-11989) allows attackers to send malicious requests that contain payloads to bypass the authentication process. In Apache Shiro 1.5.3, some measures have been taken to fix this vulnerability. However, the vulnerability still exists in later versions because Apache Shiro and Spring frameworks process URL requests in different ways. On August 17, 2020, Apache Shiro released version 1.6.0. In this version, the vulnerability is fixed. Cloud Firewall has released a virtual patch to fix this vulnerability.

Impact scope: Apache Shiro versions earlier than 1.6.0

Risk level: high

Rule-based defense: A virtual patch is available in the Cloud Firewall console to defend against this vulnerability.

Rule type: others

Security suggestions:

- Upgrade Apache Shiro to 1.6.0 or later.
- Use the Intrusion Prevention feature of Cloud Firewall.

2.[Virtual patch] Apache Dubbo remote code execution vulnerability (CVE-2020-1948)

On June 23, 2020, Alibaba Cloud emergency response center detected that Apache Dubbo announced a remote code execution vulnerability.

Apache Dubbo is a high-performance Java-based RPC framework. Apache Dubbo announced that Dubbo Provider has a remote code execution vulnerability (CVE-2020-1948) resulting from deserialization. Attackers can create and send RPC requests with malicious parameter payloads. The deserialization of malicious parameters will cause remote code execution.

Scope of impact:

- Apache Dubbo 2.7.0-2.7.6
- Apache Dubbo 2.6.0-2.6.7
- Apache Dubbo 2.5.x. Apache Dubbo will no longer provide technical support for these versions.

Risk level: high

Rule-based defense: A virtual patch is available in the Cloud Firewall console to defend against this vulnerability.

Rule type: command execution

Security suggestions:

- Apache Dubbo has released a new version 2.7.7 to fix this vulnerability. You can upgrade your Apache Dubbo version to 2.7.7 or later. Download URL for Apache Dubbo 2.7.7: [Download URL](#)
- Use the Intrusion Prevention feature of Cloud Firewall.

3. [\[Virtual patch\] Remote code execution vulnerability \(CVE-2020-0796\)](#) in Windows SMBv3

At 23:00 on March 12, 2020, Microsoft Security Center released a patch to fix the remote code execution vulnerability CVE-2020-5405, which affects Windows SMBv3.

The vulnerability occurred in `srv2.sys` because SMBv3 does not correctly handle compressed data packets. SMBv3 decompresses the data packets based on the length supported by the client, but does not check whether the length is valid. This results in integer overflow. If integer overflow occurs, an unauthenticated attacker can remotely construct malicious requests and execute commands on hosts that run specific Windows operating systems.

Risk level: high

Scope of impact:

- Windows Server, version 1909 (Server Core installation)
- Windows Server, version 1903 (Server Core installation)
- Windows 10, version 1903 for 32-bit systems
- Windows 10, version 1903 for x64-based systems
- Windows 10, version 1903 for ARM64-based systems
- Windows 10, version 1909 for 32-bit systems
- Windows 10, version 1909 for x64-based systems
- Windows 10, version 1909 for ARM64-based systems

Rule-based defense: A virtual patch is available in the Cloud Firewall console to address this vulnerability.

Rule type: command execution

Security suggestions:

- Install the patch issued by Microsoft. For more information, see [Description of CVE-2020-0796](#).
- Use the intrusion prevention feature of Cloud Firewall.

4.[Virtual patch] Apache Tomcat AJP file read and inclusion vulnerability

Apache Tomcat is a Servlet container developed by the Jakarta project, which is a part of the Apache Software Foundation. By default, Apache Tomcat uses AJP connectors to exchange data with other web servers.

Due to a defect in the AJP protocol, attackers can use AJP connectors to read or include all files in the *webapp* directory. If the target application allows for file uploads, attackers can upload malicious code and execute it remotely. Attackers can exploit this vulnerability if the AJP service is enabled and the service port is exposed. (By default, Apache Tomcat enables the AJP service and binds the service port to *0.0.0.0*.)

Scope of impact: Tomcat 6.x.x, 7.x.x, 8.x.x, and 9.x.x with the AJP service enabled

Risk level: high

Rule-based defense: A virtual patch is available in Cloud Firewall to address this vulnerability.

Rule type: command execution

Security suggestions: Upgrade Apache Tomcat or use the intrusion prevention function in Cloud Firewall to protect your servers.

5.[Threat intelligence] Apache Dubbo deserialization vulnerability (CVE-2019-17564)

On February 11, 2020, Alibaba Security Response Center (ASRC) detected an Apache Dubbo deserialization vulnerability (CVE No.: CVE-2019-17564).

Apache Dubbo is a Java-based, distributed remote procedure call (RPC) framework. It supports various protocols and is widely used. We recommend that you use the officially offered Dubbo protocol. Apache Dubbo allows you to use the HTTP protocol for RPC, which is implemented by using Spring HttpInvoker. Deserialization is performed when input streams are processed. When HTTP is enabled, Apache Dubbo performs insecure deserialization upon receiving a remote call request. This leads to the remote execution of arbitrary code.

Cloud Firewall has detected attacks that are initiated by using this vulnerability and blocks such attacks.

Affected versions: Apache Dubbo versions earlier than 2.7.5

Risk level: high

Suggestion: Use the Intrusion Prevention feature of Cloud Firewall.

6. [Virtual patch] Remote command execution vulnerability (CVE-2020-7799) in FusionAuth

FusionAuth is an open-source access management application that can be integrated with various technologies and platforms. You can configure and customize FusionAuth in a variety of ways by managing dashboards. FusionAuth can provide identity authentication, authorization, and user management for any applications.

In FusionAuth versions earlier than 1.11, the Apache FreeMarker template engine is used and user input is not filtered. When a user edits an email template, the user can use the Apache FreeMarker template engine to call `freemarker.template.utility.Execute` and execute any commands in the underlying operating system.

Scope of impact: FusionAuth 1.10.1 and earlier

Rule-based defense: Cloud Firewall has created a solution to address the vulnerability through basic rules.

Rule type: command execution

Risk level: high

Security suggestions:

- Upgrade FusionAuth.
- Use the Intrusion Prevention feature of Cloud Firewall.

7.[Basic rule] Remote code execution vulnerability in e-cology

Alibaba Cloud Cloud Firewall has created a solution to address the remote code execution vulnerability in e-cology.

e-cology is a collaborative management software developed by Weaver.

On September 19, 2019, Alibaba Cloud emergency response center detected a remote code execution vulnerability in e-cology. Attackers can create specific HTTP requests to obtain operation permissions on the target server and then remotely execute commands without authorization.

Cause of the vulnerability: e-cology has a BeanShell component that allows unauthorized access. Attackers can call the BeanShell component API to execute commands on the target server.

Rule-based defense: Cloud Firewall has created a solution to address the vulnerability through basic rules.

Rule type: command execution

Risk level: high

Security suggestions:

- Contact Alibaba Cloud to obtain a security upgrade solution.
- Use the intrusion prevention feature of Cloud Firewall.

8.[Virtual patch] Remote command execution vulnerability in Nexus Repository Manager 2.x (CVE-2019-5475)

Sonatype Nexus Repository Manager (NXRM) is a Maven repository manager developed by Sonatype.

On September 6, 2019, Alibaba Cloud emergency response center detected a remote command execution vulnerability in Nexus Repository Manager 2.x. Attackers can log on to Nexus Repository Manager 2.x Capabilities through HTTP Basic Authentication and by using the default account and password: `admin:admin123`. After logon, attackers can run the `createrepo` or `mergerepo` command to implement remote system command injection. Attackers can exploit this vulnerability to remotely execute server commands, causing great risks.

Scope of impact: Nexus Repository Manager OSS and Nexus Repository Manager Pro in versions earlier than 2.14.14

Rule-based defense: A virtual patch is available in the Cloud Firewall console to address this vulnerability.

Rule type: command execution

Risk level: high

Security suggestions: Upgrade Nexus Repository Manager 2.x to version 2.14.14.

9.[Threat intelligence] Remote code execution vulnerability (CVE-2019-0708) in Windows RDP

On September 6, 2019, Alibaba Cloud emergency response center detected that Metasploit released an exploit module for BlueKeep (CVE-2019-0708). The Alibaba Cloud security team has confirmed that the exploit module can be successfully executed. With the EXP code, attackers can execute any commands on the target system and spread worms to infect other hosts on the internal network. The BlueKeep vulnerability is similar to ransomware such as WannaCry in 2017 and causes high risks.

The public release of the exploit module greatly lowers the vulnerability exploitation threshold and makes hosts with the BlueKeep vulnerability prone to intrusion. Alibaba Cloud reminds Windows users to check for vulnerabilities and fix them in a timely manner.

Scope of impact:

- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows 2003
- Windows XP

Risk level: high

Security suggestions:

1. Fix vulnerabilities in a timely manner. For more information about fixing the vulnerabilities, see [Microsoft security announcement](#).
2. Use Cloud Firewall ACL to restrict RDP. For more information, see [Overview of access control policies](#). We recommend that you use an IP address whitelist to allow access to resources.

10.[Virtual Patches] Remote code execution vulnerability in Redis 4.0 and Redis 5.x

On July 9, 2019, Alibaba Cloud Security detected a remote code execution vulnerability in Redis 4.0 and 5.x versions. A new function module was added to Redis 4.0, and is enabled by default in later versions. Users can use C language to compile a `.so` file to execute system commands, which brings high risks.

On July 9, 2019, Cloud Firewall released a virtual patch for this vulnerability. We recommend that Redis users enable this virtual patch.

Impacted versions: Redis 4.0, Redis 5.0 and later

Policy: command execution

Risk level: high

Policy-based protection: A virtual patch is available in the Cloud Firewall console to defend against this vulnerability.

11.[Virtual Patches] Remote command execution vulnerability in Seeyon OA system

On June 26, 2019, Alibaba Cloud Security detected a remote command execution vulnerability in Seeyon office automation (OA) system. The htmlofficeservlet interface of Seeyon OA system has a vulnerability in processing specific requests. Attackers may send specially crafted HTTP requests to exploit the vulnerability and execute arbitrary commands on the target server. This is a high-risk vulnerability. Alibaba Cloud Security has figured out how this 0-day vulnerability is exploited.

On June 27, 2019, Cloud Firewall released a virtual patch to address this vulnerability. We recommend that you enable virtual patches (enabled by default when the Cloud Firewall service is activated) and traffic control mode for protection. Seeyon has released an official security patch. Users can contact Seeyon for system updates.

Impacted system: Seeyon OA system

Policy: command execution

Risk level: high

Policy-based protection: A virtual patch is available in the Cloud Firewall console to address this vulnerability.

12.[Virtual Patches] Remote code execution vulnerability (CVE-2019-0708) in Windows RDP

On May 15, 2019, Microsoft released security updates to address a remote code execution vulnerability (CVE-2019-0708) in Remote Desktop Services. This vulnerability has negatively impacted some earlier Windows versions.

User authentication is not required in this vulnerability exploitation. Unauthenticated users may use RDP port 3389 to connect with the target server and send specially crafted requests. This enables the users to execute arbitrary commands on the target server or spread worms to infect other servers in the internal network.

On May 22, 2019, Cloud Firewall released a virtual patch to address this vulnerability. We recommend that you enable this virtual patch (enabled by default when Cloud Firewall service is activated) and traffic control mode for protection.

Impacted versions:

- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows 2003
- Windows XP

Policy: command execution

Risk level: high

Policy-based protection: A virtual patch is available in the Cloud Firewall console to address this vulnerability.

Security tips

1. We recommend that users of Windows 7, Windows Server 2008, and Windows Server 2008 R2 install the [Windows security patch](#).
2. We recommend that users of Windows 2003 and Windows XP update the system or install the [Windows security patch](#).
3. Log on to the Cloud Firewall console. Choose **Security Policies > Intrusion Prevention**, and enable the [Intrusion prevention policies](#) feature.
4. In the Cloud Firewall console, choose **Security Policies > Access Control > Internet Firewall > Inbound Policies**. Create an access control policy that allows only trusted sources or denies all requests from regions except the trusted regions.

13.[Virtual patch] WebLogic wls9-async deserialization remote command execution

On April 17, 2019, Yundun emergency response center of Alibaba Cloud detected the vulnerability named as "Oracle WebLogic wls9-async deserialization remote command execution vulnerability" disclosed by China National Vulnerability Database (CNVD). Attackers can exploit this vulnerability to remotely execute commands without authorization.

The default wls9_async_response package in some WebLogic versions provides asynchronous communication services for WebLogic Server. Because the War package has a defect in deserializd information processing, attackers can send specially crafted malicious HTTP requests to obtain the permissions of the target server and remotely execute commands without authorization.

Scope of impact: Oracle WebLogic 10. X and Oracle WebLogic 12.1.3

Risk level: High risk

Policy-based protection: Cloud Firewall provides virtual patches to fix this vulnerability. We recommend that you enable the Virtual Patches in [Intrusion Prevention](#) to defend against this vulnerability.

14.[Threat notice] Unauthorized access to MongoDB

Unauthorized access to MongoDB could lead to data disclosure or deletion extortion, which could have grave consequences.

For example, on February 14, 2019, the National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC) detected that some MongoDB databases in China were exposed on the Internet, leading to leaks of important information.

Hazards:

By default, a MongoDB database requires no authentication if you do not set any parameters when activating the MongoDB service. Without any passwords, users who have logged on to the service can use the default port to remotely access the database and perform any operations (including high-risk operations such as add, delete, edit, and query) on the database.

To ensure the security of your business and applications, fix the vulnerability as soon as possible. For more information, see [Best practices for defense against unauthorized access to MongoDB](#).

15. Confluence remote file reading vulnerability (CVE-2019-3396)

Confluence is a professional enterprise knowledge management and collaboration software that can be used to build an enterprise wiki.

On July 6, April 4, 2019, Yundun emergency response center of Alibaba Cloud detected the official security update released by Confluence, because Widget Connector has the server template injection vulnerability. Attackers can exploit this vulnerability to implement directory traversal and even remote command execution.

Recently, Alibaba Cloud detected the latest vulnerability exploitation method, and multiple worms began to exploit this vulnerability for dissemination.

Rule type: Command execution

Risk level: High risk

Secure version:

- Version 6.6.12 and higher versions of 6.6.x
- Version 6.12.3 and higher versions of 6.12.x
- Version 6.13.3 and higher versions of 6.13.x
- Version 6.14.2 and higher

Policy-based protection: Cloud Firewall provides virtual patches to fix this vulnerability. We recommend that you enable the Virtual Patches in [Intrusion Prevention](#) to defend against this vulnerability.

16.[Threat Intelligence] Attacks on Jenkins

On February 28, 2019, Alibaba Cloud Security discovered that many methods of exploiting Jenkins vulnerabilities were revealed online, and most of the vulnerabilities were high-risk RCE vulnerabilities. Attackers use various types of worms to increase the number of Jenkins RCE vulnerabilities.

The following vulnerabilities have been exploited frequently: CVE-2019-1003000, CVE-2019-1003001, CVE-2015-5323, CVE-2015-1814, CVE-2016-0792, and CVE-2017-1000353. These vulnerabilities exist in multiple Jenkins versions and plug-ins.

Risk level: High

Policy-based protection: Cloud Firewall provides virtual patches to fix this vulnerability. We recommend that you enable the Virtual Patches in [Intrusion Prevention](#) to defend against this vulnerability.

17.[Virtual Patches] Remote code execution vulnerability in Nexus Repository Manager 3 (CVE-2019-7238)

Nexus Repository Manager (NXRM) is a software package repository management service developed by Sonatype. NXRM can be used as a private Maven server.

Vulnerabilities have been detected in some versions of Nexus Repository Manager, and no vulnerability fix is available. Unauthorized users can exploit this vulnerability to construct specific requests to remotely execute Java code on the NXRM server.

Vulnerability description: [CVE-2019-7238 Nexus Repository Manager 3 \(Missing Access Controls and Remote Code Execution\) - February 5th 2019](#)

Policy: Command execution

Risk level: High

Impacted versions: Nexus Repository Manager OSS/Pro 3.6.2 to 3.14.0

Policy-based protection: Cloud Firewall provides virtual patches to fix this vulnerability. We recommend that you enable [Intrusion Prevention](#) to avoid this vulnerability.

18.[Basic Policies] Remote code execution vulnerability in Jenkins (CVE-2019-1003000)

Jenkins is an open-source program written in Java. It can be used as a continuous integration server. The Script Security and Pipeline plug-in is a security plug-in of Jenkins and can be integrated into various functional plug-ins of Jenkins.

Alibaba Cloud Security has discovered that the exploitation methods of the remote code execution vulnerability in Jenkins Script Security and Pipeline (CVE-2019-1003000) have been revealed on the Internet. Users with overall or read permissions can bypass sandbox protections and execute arbitrary code in Jenkins.

Vulnerability description: [Jenkins Security Advisory 2019-01-08](#)

Policy: Command execution

Risk level: High

Impacted plug-ins:

- Declarative Plug-in versions earlier than 1.3.4.1
- Groovy Plug-in versions earlier than 2.61.1
- Script Security Plug-in versions earlier than 1.5.0

Policy-based protection: Cloud Firewall provides basic firewall policies to fix this vulnerability. We recommend that you enable [Intrusion Prevention](#) to use the basic policies.

19.[Virtual patch] User privilege escalation vulnerability in Kubernetes (CVE-2018-1002105)

Kubernetes is commonly stylized as K8s, which is an abbreviation derived by replacing the eight letters "ubernete" with an 8. K8s is an open-source system for managing containerized applications across multiple hosts deployed on the cloud platform.

With a specially crafted request, a normal K8s user who has established a connection through the K8s API server to a backend server can perform privilege escalation. To do so, the normal user must have the `exec/attach/portforward` permissions on at least one pod. The attacker can then send arbitrary requests over the established connection directly to that backend server to gain full admin privileges (including root privileges) on all nodes in a K8s cluster.

Servers using affected K8s versions are at high risk of intrusions. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

Rule type: Command execution

Risk level: High

Scope of impact:

- Kubernetes v1.0.x to 1.9.x
- Kubernetes v1.10.0 to 1.10.10 (fixed in v1.10.11)
- Kubernetes v1.11.0 to 1.11.4 (fixed in v1.11.5)
- Kubernetes v1.12.0 to 1.12.2 (fixed in v1.12.3)

Rule-based defense: A virtual patch is available in the Cloud Firewall console to defend against this vulnerability.

20.[Basic rule] Remote code execution vulnerabilities in multiple versions of ThinkPHP 5.1 series and 5.2 series

On January 15, 2019, Alibaba Cloud Security team detected remote code execution vulnerabilities in all versions of ThinkPHP 5.1 series and 5.2 series under certain conditions.

These vulnerabilities are caused by a flaw in the process of handling methods of the Request class by the ThinkPHP 5.0 framework. Hackers exploit these vulnerabilities to create special requests to obtain webshell directly.

In the past two months, multiple high-risk command execution vulnerabilities in the ThinkPHP5 framework have been continuously disclosed. Cloud Firewall has launched rules for defending against these vulnerabilities. Cloud Firewall can monitor and intercept the attacks exploiting these vulnerabilities in real time.

Rule type: Web attack

Risk Level: High

Scope of impact: All versions of ThinkPHP 5.1 series and 5.2 series

Rule-based defense: Cloud Firewall has been able to defend against these vulnerabilities. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

21.[Basic rule] Remote code execution vulnerabilities in ThinkPHP versions earlier than 5.0.24

ThinkPHP is a simple, fast, and compatible lightweight PHP development framework, which Chinese websites use widely, especially in the e-commerce, financial service, and online gaming industries.

On January 11, 2019, ThinkPHP team officially released a security update that disclosed a high-risk security vulnerability: Attackers can create special malicious requests to obtain server privileges directly.

These vulnerabilities are caused by a flaw in the process of handling methods of the Request class by the ThinkPHP 5.0 framework. Hackers exploit these vulnerabilities to create special requests to obtain webshell directly.

ThinkPHP versions from 5.0.0 to 5.0.23 are affected.

Rule-based defense: Cloud Firewall has been able to defend against these vulnerabilities.

Scope of impact: ThinkPHP v5.0 series versions earlier than 5.0.24

Rule type: Web attack

Risk level: High

22.[Basic rule] Malicious file writing vulnerability of PostgreSQL

Alibaba Cloud's Cloud Firewall has been able to defend against the malicious file writing vulnerability of PostgreSQL.

PostgreSQL is a powerful, open-source object-relational database that runs on multiple operating systems. The PostgreSQL function `Lo_export` can be called to export large objects to a file. Once an attacker obtains PostgreSQL database privileges, the attacker can use the `Lo_import` and `Lo_export` functions to import malicious library files and execute system commands.

Rule type: Command execution

Risk level: High

Scope of impact: PostgreSQL databases

Rule-based defense: Cloud Firewall has been able to defend against this vulnerability. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

23.[Threat intelligence] Multiple botnets exploit the ThinkPHP v5 vulnerability

Alibaba Cloud's Cloud Firewall has been able to defend against the attacks from multiple botnets that exploit the ThinkPHP v5 vulnerability.

Recently, Alibaba Cloud Security team detected that several cryptocurrency miner botnets have begun to exploit the new ThinkPHP vulnerability to propagate themselves. BuleHero is a botnet that exploits multiple security vulnerabilities and controls Windows servers to mine cryptocurrency, posing critical security threats to business. Systems with the ThinkPHP v5 vulnerability are prone to infection by BuleHero and Sefa. Once a system is infected, worms are spread on internal networks, posing critical security threats to enterprises' internal networks. BuleHero and Sefa can also control servers to mine cryptocurrency, affecting the normal running of business.

For more information about the threat and the malicious links, see [Threat Alert: Multiple Cryptocurrency Miner Botnets Start to Exploit the New ThinkPHP Vulnerability](#).

Rule type: Worm attack

Risk level: High

Cloud Firewall has been able to defend against such attacks. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

24.[Virtual patch] ThinkPHP 5.x remote command execution (getshell)

Cloud Firewall has been able to defend against ThinkPHP 5.x remote command execution (getshell) attacks.

ThinkPHP is a simple, fast, and compatible lightweight PHP development framework, which Chinese websites use widely, especially in the e-commerce, financial services, and online gaming industries.

On December 10, 2018, the ThinkPHP team released a patch to fix a remote code execution vulnerability caused by the ThinkPHP v5 framework's insufficient checks on controllers. That vulnerability can be widely used to execute any code and commands remotely. Security checks on controller names in the ThinkPHP v5 framework are insufficient. If no forced routing has been configured, hackers can exploit the vulnerability to create special requests to run code remotely and get server privileges.

Scope of impact: ThinkPHP v5.0 series earlier than 5.0.23 and ThinkPHP v5.1 series earlier than 5.1.31

Rule type: Web attack

Risk level: High

Rule-based defense: Cloud Firewall has been able to defend against such attacks. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

25.[Basic rule] Update of Bash reverse shell detection rules

Cloud Firewall has updated the Bash reverse shell detection rules.

A lot of cyberattacks are launched by exploiting reverse shells. Such attacks often occur during the maintenance stage. Once an attacker obtains certain system command execution privileges, the attacker can use a reverse shell to open an interactive command execution window and then intrude into the system to steal data. When Cloud Firewall detects a reverse shell attack to your server, indicating that your server is at risk of intrusion, it blocks the reverse shell creation and command execution. This helps reduce the risks that the attack may bring.

Rule type: Reverse shell

Risk level: High

Rule-based defense: Cloud Firewall has been able to defend against such attacks. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

26.[Basic rule] Update of mining pool communication detection rules

Alibaba Cloud's Cloud Firewall has updated the mining pool communication detection rules.

With the rise of cryptocurrencies such as bitcoin, security events for the sake of profits by cryptocurrency mining are increasingly rampant. More and more servers are attacked for cryptocurrency mining. Once a computer is infected with a mining Trojan, it becomes a profitable tool for hackers, and the computer resources become exhausted. This brings serious impact on normal business. Recently, Cloud Firewall updated the mining pool communication detection rules. After the update, Cloud Firewall is able to detect the servers that hackers are using to mine cryptocurrency.

Rule type: cryptocurrency mining

Risk level: High

Cloud Firewall has been able to detect cryptocurrency mining. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

27.[Basic rule] PHPCMS 2008 code injection vulnerability (CVE-2018-19127)

PHPCMS is a mainstream content management system used in China. It is an open-source PHP development framework. PHPCMS was first released in 2008, and the latest version is v9.6.3. Many websites are still using PHPCMS 2008 for its stable, flexible, and open-source. However, PHPCMS 2008 is prone to a code injection vulnerability (CVE-2018-19127). This vulnerability allows attackers to write arbitrary content to a website cache file with a controllable filename, leading to arbitrary code execution.

Recently, Alibaba Cloud Security team detected multiple samples of the PHPCMS 2008 code injection vulnerability.

Rule-based defense: Cloud Firewall has been able to defend against this vulnerability. We recommend that you enable intrusion prevention policies in the Cloud Firewall console.

Scope of impact: PHPCMS 2008

Rule type: Command execution

Risk level: High

28.[Virtual patch] WebLogic T3 deserialization vulnerability

In April, 2018, Oracle officially released a Critical Patch Update, which is a collection of patches for multiple security vulnerabilities including the high-risk WebLogic T3 deserialization vulnerability (CVE-2018-2628). Attackers can exploit this vulnerability to execute code remotely without authorization. This vulnerability brings high security risks. Oracle officially released the latest patch in a timely manner to fix the vulnerability. You are advised to perform a self-check and upgrade immediately.

The WebLogic T3 protocol deserialization vulnerability on Oracle WebLogic Server 10.3.6.0, 12.1.3.0, 12.2.1.2, and 12.2.1.13 may lead to remote code execution. A malicious attacker can remotely execute commands by constructing malicious request packets to obtain system privileges, which brings serious security risks.

CVE code: CVE-2018-2628

Rule-based defense: Cloud Firewall has been able to defend against remote command execution caused by this vulnerability.

Scope of impact: WebLogic 10.3.6.0, 12.1.3.0, 12.2.1.2, and 12.2.1.3

Rule type: Command execution

Risk level: High

29.[Threat intelligence] Redis unauthorized access vulnerability

On September 12, 2018, the Alibaba Cloud Security team detected a large number of worm propagation incidents exploiting the authorized access vulnerability of Redis. Servers infected by worms launched the attacks.

Command-and-control server IP address: 104.20.208.21

The controlled servers access <https://pastebin.com/raw/5bjpvyLP> to download malicious files and spread the worm to recipients.

Malicious IP address: 104.20.208.21

Event: Redis worm from a command-and-control server

Risk level: High

30.[Basic rule] Remote command execution through Microsoft SQL Server xp_cmdshell

SQL Server is a relational database management system introduced by Microsoft Corporation. The extended stored procedure xp_cmdshell of SQL Server is used to run system commands. The xp_cmdshell option enables system administrators to control whether to spawn a Windows command shell and pass it in a string for execution. Any output is returned as rows of text.

Malicious users sometimes attempt to elevate their privileges by using xp_cmdshell to run system commands.

Rule-based defense: Cloud Firewall has been able to defend against remote command execution through SQL Server xp_cmdshell.

Scope of impact: Microsoft SQL Server

Rule type: Command execution

Risk level: High

31.[Virtual patch] Nginx security issues cause servers' vulnerability to DoS attacks

Nginx has been experiencing security issues recently, which may cause more than 14 million servers to be vulnerable to DoS attacks. The vulnerabilities that cause the security issues are in the HTTP/2 and MP4 modules.

Two security vulnerabilities were identified in Nginx HTTP/2 implementation. Nginx compiled with the ngx_http_v2_module (not compiled by default) is affected if the http2 option of the listen directive is used in a configuration file. This may cause excessive memory consumption (CVE-2018-16843) and CPU usage (CVE-2018-16844).

To take advantage of these two vulnerabilities, an attacker can send a specially crafted HTTP/2 request, which results in excessive CPU usage and memory usage, eventually triggering a DoS status. All Nginx servers that are running unpatched versions are vulnerable to DoS attacks.

Scope of impact:

- CVE-2018-16843 and CVE-2018-16844: Mainline versions 1.9.5 - 1.15.5
- CVE-2018-16845: Mainline versions 1.1.3+ and 1.0.7+

Rule type: DoS attack

Risk level: High

Rule-based defense: Cloud Firewall has been able to use the virtual patch feature to defend against such attacks. For more information about the virtual patch feature, see [Virtual patching](#).

For more information about the alert, see [Nginx security issues cause over 14 million servers to be vulnerable to DoS attacks](#).

32.[Threat intelligence] QBotVariant attack

In May 2018, the Alibaba Cloud Security team detected worm samples written based on the QBot open-source code. Further investigation revealed that this was indeed a new QBot family member, which the team named QBotVariant. QBotVariant is capable of performing DDoS attacks, leveraging backdoors and downloaders, and conducting brute-force cracking. Infected servers become part of the QBotVariant botnet. QBotVariant can spread widely on the Internet and cause great harm.

QBotVariant exploits the REST API unauthorized access vulnerability of Hadoop YARN and uses hard-coded weak passwords to perform brute-force cracking. Once a server is infected, it becomes a botnet member that attacks other servers, and its bandwidth is consumed by its new "master." Furthermore, this infection may result in consequences such as data leakage and data loss.

Event: Worm attack

Risk level: High

Cloud Firewall has been able to defend against such attacks. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

For more information, see [Some malicious URLs and QBotVariant details](#).

33.[Threat intelligence] DDG mining botnet attack

DDG is a Monero-mining botnet that targets Redis servers through brute-force attacks against SSH and unauthorized access vulnerability. The latest DDG version is 3014.

Recently, Alibaba Cloud Security team detects an increase in the number of DDG mining botnet attacks. Once an attack succeeds, DDG executes the crontab command on the controlled servers to perform regularly update and run. Update source: `hxxp://149.56.106.215:8000/i.sh`

Download URLs:

- `hxxp://149.56.106.215:8000/i.sh`
- `hxxp://149.56.106.215:8000/static/3014/ddgs.i686`
- `hxxp://149.56.106.215:8000/static/3014/ddgs.x86_64`

Malicious IP address: 149.56.106.215

Event: DDG worm from a command-and-control server

Risk level: High

Cloud Firewall has been able to defend against such attacks. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

34.[Basic rule] Malicious MySQL UDF execution

MySQL allows users to specify user-defined functions (UDFs). Attackers who have MySQL database privileges can exploit this vulnerability to import custom UDFs from malicious library files to execute system commands.

This vulnerability mainly affects opened MySQL application servers. It may cause risks such as unauthorized control over servers, data leakage, ransom, cryptocurrency mining, and Distributed Denial of Service (DDoS) attacks to external systems.

Rule-based defense: Cloud Firewall has been able to defend against this vulnerability. We recommend that you enable [intrusion prevention policies](#) in the Cloud Firewall console.

Scope of impact: MySQL databases

Rule type: Command execution

Risk level: High

35.[Virtual patch] Arbitrary file upload vulnerability of WebLogic (CVE-2018-2894)

Alibaba Cloud's Cloud Firewall has been able to defend against the arbitrary file upload vulnerability of WebLogic.

WebLogic is an application server launched by Oracle Corporation, which is a piece of middleware based on the Java EE architecture. The WebLogic Java application server is used to develop, integrate, deploy, and manage large distributed web applications, network applications, and database applications.

The configuration page of `ws_utc`, a WebLogic web service test client, has an issue of unauthorized access. The path to the configuration page is `/ws_utc/config.do`. Attackers can access this configuration page, use a valid WebLogic web path to replace the JKS Keystores file path, and upload malicious JSP Trojan files.

Rule-based defense: Cloud Firewall has been able to defend against this vulnerability.

Scope of impact:

- WebLogic 10.3.6.0
- WebLogic 12.1.3.0
- WebLogic 12.2.1.2
- WebLogic 12.2.1.3

Rule type: Command execution

Risk level: High

36.[Threat intelligence] REST API unauthorized access vulnerability of Hadoop YARN

Alibaba Cloud's Cloud Firewall has been able to defend against the REST API unauthorized access vulnerability of Hadoop YARN.

Hadoop is a distributed system framework developed by the Apache Software Foundation. It uses the well-known MapReduce algorithm to implement distributed processing. YARN serves as a resource management system for Hadoop clusters. Improper configuration of Hadoop YARN may lead to unauthorized access, which attackers can exploit. Without authentication, attackers can deploy tasks to run commands through a REST API, and ultimately gain full control over servers.

On October 25, 2018, Cloud Firewall detected a large number of attacks that exploited this vulnerability. Once the attack succeeds, the controlled servers access `hxxps://bitbucket.org/*/raw/master/zz.sh` to download malicious files for cryptocurrency mining.

Cloud Firewall has been able to defend against such attacks.

Event: REST API unauthorized access vulnerability of Hadoop YARN

Risk level: High