Web Application Firewall

Release Notes and Announcements

Product Documentation

©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Release Notes and Announcements
- Release Notes
- Product Announcement
  - Adjusting Billing of WAF BOT Traffic Management
  - Announcements
- Security Advisory
  - Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-44832)
  - Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-45046)
  - Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-44228)
  - Notice for WebLogic Console HTTP RCE Vulnerability
  - Notice for Exchange Server Command Execution Vulnerability
  - Notice for Yonyou GRP-U8 SQL Injection Vulnerability
  - Notice for Apache Cocoon XXE Vulnerability (CVE-2020-11991)
  - Notice for WordPress File Manager Arbitrary Code Execution Vulnerability
  - Jenkins Security Advisory for September
  - Notice for Apache Struts 2 RCE Vulnerabilities (CVE-2019-0230 and CVE-2019-0233)
  - Notice for Apache SkyWalking SQL Injection Vulnerability (CVE-2020-13921)

©2013-2022 Tencent Cloud. All rights reserved.

Release Notes and Announcements

Release Notes

Last updated：2022-06-23 11:14:26

June 2022

Update	Description	Release Date	Documentation
Experience upgrade	WAF instance data storage outside the Chinese mainland is optimized, which supports the isolation and display of resource data by region, improving the user operation and management experience.	2022-06-03	-
Operation log	You can view WAF operation logs recorded by CloudAudit in the console and perform queries and backtracking.	2022-06-03	-
Instance list	You can purchase WAF instances on different editions or upgrade instances across editions to protect your businesses as needed.	2022-06-03	-
Connection mode	You can configure multi-IP weighted round robin permissions in the origin-pull mode to meet the requirements of complex SaaS business	2022-06-03	-

©2013-2022 Tencent Cloud. All rights reserved.

	connection for load balancing.		
IP blocking capability enhancement	Domain name-based IP blocking is supported to implement more refined protection.	2022-06-03	-
Regional blocking	Regional blocking can be quickly configured to improve the access control configuration experience.	2022-06-03	-
Quick protection switch	You can quickly enable or disable all protection modules and certain features of certain protection modules. This facilitates routine Ops troubleshooting, accelerates problem locating, and ensures business continuity.	2022-06-03	-
Refined traffic management	IP blocklist/allowlist is upgraded to blocklist/allowlist management. Custom policy rules that were previously set to "allow" are upgraded to precise allowlist rules, and other custom policy rules are upgraded to access control rules. Rule configuration and execution are not affected by the upgrade. The precise allowlist feature implements refined traffic management during routine security Ops, improving the traffic control efficiency and	2022-06-03	-

©2013-2022 Tencent Cloud. All rights reserved.

	effect while ensuring business security.		
Log service	After purchasing the value-added log service, you can enable the real-time storage and query of all access logs.	2022-06-03	-
Custom traffic tagging	Custom traffic tagging is supported to meet the requirements of more complex business analysis and linked protection.	2022-06-03	-
Domain name connection guide	A domain name connection guide is added, providing more detailed directions after a domain name is added and facilitating business connection.	2022-06-03	-
Comprehensive bot protection	The bot protection feature is upgraded comprehensively to support capabilities such as the browser bot defense module, threat intelligence module, AI evaluation module, score-based bot traffic identification, and visualized traffic analysis.	2022-06-03	-
Bot report	You can quickly spot bot threats to your website, specific APIs under attacks, and bot-targeted resources, so that you can respond immediately with bot countermeasures and	2022-06-03	-

©2013-2022 Tencent Cloud. All rights reserved.

	protect your website business.		

©2013-2022 Tencent Cloud. All rights reserved.

Product Announcement
Adjusting Billing of WAF BOT Traffic Management

Last updated：2023-09-08 18:22:07

WAF plans to adjust the billing of BOT traffic management fees starting from October 11, 2023.
Updates are as follows:
Before adjustment: The BOT traffic management fee is billed independently from the WAF instance, with a quota of 2500 QPS per month. For out-of-plan QPS, you can purchase extra packages (750 USD/1000 QPS/month).
After adjustment: The BOT traffic management fee is billed together with the WAF instance. It shares the QPS quota of the WAF instance. The QPS quota varies by the instance edition. The selling of extra packages for BOT traffic management stops. For out-of-plan QPS, you can purchase extra capacity packages at a price of 275 USD/1000 QPS/month (for Chinese mainland regions) or 300 USD/1000 QPS/month (for regions outside the Chinese mainland).
The above policy starts canary release gradually from September 2023, and will be officially launched from October 11, 2023. Thanks for your support. If you have any questions, please contact us.

©2013-2022 Tencent Cloud. All rights reserved.

Announcements

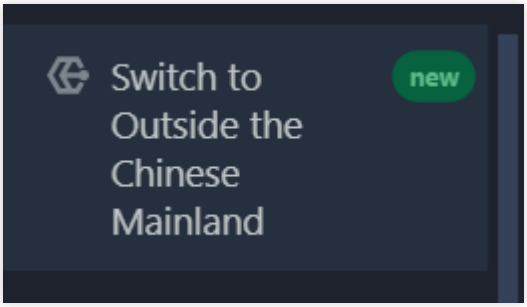
Last updated：2022-09-19 10:36:43

Release Notes at Tencent Cloud International

To improve the business connection and protection configuration experience outside the Chinese mainland, WAF was upgraded on June 2, 2022, with the web console 2.0 released. After the upgrade, connection is more stable, protection is more powerful, and traffic management is more refined, with value-added capabilities of bot traffic management and log service supported. In addition, the console allows you to switch between regions in and outside the Chinese mainland to better manage instance resources by region.
Different types of WAF instances are impacted as follows:
SaaS WAF: The region attributes of WAF instances remain unchanged, the system automatically adds region fields according to the attributes, and the console supports management by region.
CLB WAF: WAF instances in the Chinese mainland support connecting and protecting web businesses for CLB instances in the Chinese mainland, and those outside the Chinese mainland support those of CLB instances outside the Chinese mainland.
After **this** upgrade to web console 2.0, you can enjoy the following product capabilities and configurations:

Cross-region resource data isolation

The console allows you to switch between regions in and outside the Chinese mainland as shown below:



©2013-2022 Tencent Cloud. All rights reserved.

More convenient domain name connection

Upgraded domain name connection and management

You can manage multiple instances in a unified manner to improve the routine security Ops efficiency. SaaS WAF instances support custom weight-based IP forwarding as well as multi-domain name forwarding to enable complex business connections.

Domain name connection guide

A domain name connection guide is added, providing more detailed directions after a domain name is added and facilitating business connection.

Custom traffic tagging

SaaS WAF instances support custom traffic tagging to meet the requirements of more complex business analysis and linked protection.

Client information logging

SaaS WAF instances allow you to enable the transfer of business client source IP address and port information. This complements XFF records to ensure business compliance in finance and ecommerce industries.

Protection capability upgrade

Quick protection switch

You can quickly enable or disable all protection modules and certain features of certain protection modules. This facilitates routine Ops troubleshooting, accelerates problem locating, and ensures business continuity.

Refined traffic management

IP blocklist/allowlist is upgraded to blocklist/allowlist management. Custom policy rules that were previously set to "allow" are upgraded to precise allowlist rules, and other custom policy rules are upgraded to access control rules. Rule configuration and execution are not affected by the upgrade.

©2013-2022 Tencent Cloud. All rights reserved.

The precise allowlist feature implements refined traffic management during routine security Ops, improving the traffic control efficiency and effect while ensuring business security.

Value-added capability upgrade - commercial release of bot traffic management

The newly upgraded bot protection system integrates the browser bot defense module, threat intelligence module, as well as big data and AI algorithm model and analysis engine. It provides visualized traffic analysis by risk level and more intuitive threat handling policies.

©2013-2022 Tencent Cloud. All rights reserved.

Security Advisory
Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-44832)

Last updated：2022-06-23 11:14:26

On December 29, 2021, Tencent Cloud Security Operations Center noticed that **Apache Log4j 2 announced that there was a remote code execution vulnerability (CVE-2021-44832) in some special scenarios. The vulnerability is hard to exploit, as attackers can remotely execute arbitrary code only if they have permissions to modify the configuration file.**

To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Vulnerability Details

Apache Log4j 2 is an open-source Java-based logging framework. As an upgraded version of Log4j 1.x, it rewrites the Log4j framework and introduces various new features, making it widely suitable for logging in the development of many business systems.

As described by Apache, attackers with permissions to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code

As this vulnerability requires that attackers have the permission to modify configuration files (which usually can be implemented only through other vulnerabilities) and doesn't exist in the default configuration, it is hard to exploit.

Risk Level

Medium.

Vulnerability Risk

This vulnerability may be exploited by attackers to remotely execute arbitrary code.

Affected Versions

©2013-2022 Tencent Cloud. All rights reserved.

2.0-beta7 ≤ Apache Log4j 2.x < 2.17.0 (excluding 2.3.2 and 2.12.4)

Safe Versions

- Apache Log4j 2.x ≥ 2.3.2 (Java 6)
- Apache Log4j 2.x ≥ 2.12.4 (Java 7)
- Apache Log4j 2.x ≥ 2.17.1 (Java 8 or later)

Suggestions for Fix

Currently, an official safe version of Apache Log4j 2 has been released. You can update to it as instructed in Download Apache Log4j 2.

> Note：
> Back up your data before upgrading to avoid accidental losses.

Tencent Security Solution

Tencent Cloud NTA rule libraries released after December 29, 2021 support detecting the Log4j 2 RCE vulnerability CVE-2021-44832.

References

For more information, see Apache Log4j Security Vulnerabilities.

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-45046)

Last updated：2022-06-23 11:14:26

On December 17, 2021, Tencent Cloud Security Operations Center noticed that **Apache Log4j's fix for CVE-2021-44228 was incomplete in non-default configurations, so the vulnerability could be exploited by attackers to launch remote code execution attacks in some special configuration scenarios.**

To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Vulnerability Details

Apache Log4j 2 is an open-source logging component as the upgrade of Apache Log4j. It controls the output format of each log and allows you to define the level of each log to control the log generation process in a more refined manner.

After disclosing the severe RCE vulnerability CVE-2021-44228 on December 9, 2021, **Apache Log4j recently disclosed another RCE vulnerability CVE-2021-45046, whose severity increased from CVSS 3.7 to CVSS 9.0. This vulnerability is caused by the incomplete fix for CVE-2021-44228 in non-default configurations. In certain scenarios such as thread context search mode, attackers can construct specific requests to execute code remotely.**

This vulnerability also affects a high number of universal applications and components around the globe, such as:
Apache Struts 2
Apache Solr
Apache Druid
Apache Flink
Apache Dubbo
Apache Kafka
Spring-boot-starter-log4j2
Elasticsearch
Logstash
...
We recommend you check and upgrade all systems or applications that use the Log4j component in time.

Risk Level

©2013-2022 Tencent Cloud. All rights reserved.

High (CVSS score: 9.0)

Vulnerability Risk

This vulnerability may be exploited by attackers to remotely execute arbitrary code.

Affected Versions

2.0-beta9 ≤ Apache Log4j 2.x < 2.16.0 (excluding 2.12.2)

Safe Versions

- Apache Log4j 2.16.0 (Java 8)
- Apache Log4j 2.12.2 (Java 7)

Suggestions for Fix

We recommend you conduct internal inspections to check whether your business applications use the Apache `log4j-core` JAR package. If the dependency is introduced and the Log4j version is among the affected versions, the vulnerability may affect your business, and you can take the following measures:

> Note：
> Back up your data before upgrading to avoid accidental losses.

Upgrading to latest official version (recommended)

Currently, officially fixed versions have been released. You can upgrade the component or update the code to this version.

- If you use Java 8, upgrade to Apache Log4j 2.16.0.
- If you use Java 7, upgrade to Apache Log4j 2.12.2.

Using other protection solutions

©2013-2022 Tencent Cloud. All rights reserved.

1. If you cannot upgrade the version currently, we recommend you run the following command to remove the `JndiLookup` class file from the `log4j-core` package and restart the service:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

2. Use a security group or firewall to restrict the affected applications from accessing the internet.

References

For more information, see Apache Log4j Security Vulnerabilities.

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Apache Log4j 2 RCE Vulnerability (CVE-2021-44228)

Last updated：2022-06-23 11:14:26

On December 9, 2021, Tencent Cloud Security Operations Center noticed that **a severe code execution vulnerability (CVE-2021-44228) in Apache Log4j 2 was disclosed. Currently, Log4j 2 has released an official security announcement and safe version. Once the vulnerability is exploited, problems such as server intrusion can occur.**

To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Vulnerability Details

Apache Log4j 2 is a widely used open-source logging component. It substitutes for print statements such as `System.out` in projects and is the most popular logging tool in Java.

If Log4j 2 is used to process malicious data in certain scenarios, malicious code may be injected and executed.

Log4j 2 is used by many Java frameworks and applications as a third-party basic logging library. Your business may be attacked through this vulnerability if it uses Log4j 2 to output logs and the log content can be partially controlled by attackers. Therefore, this vulnerability also affects a high number of universal applications and components around the globe, such as:
Apache Struts 2
Apache Solr
Apache Druid
Apache Flink
Apache Flume
Apache Dubbo
Apache Kafka
Spring-boot-starter-log4j2
Elasticsearch
Logstash
...
We recommend you check and upgrade all systems or applications that use the Log4j component in time.

©2013-2022 Tencent Cloud. All rights reserved.

Risk Level

High Risk

Vulnerability Risk

This vulnerability may be exploited by attackers to remotely execute arbitrary code.

Affected Versions

Apache Log4j 2.0–2.14.1

Safe Versions

Apache Log4j 2.16.0

Suggestions for Fix

Upgrading to latest official version (recommended)

The current latest official version is log4j-core-2.16.0. You can upgrade the component or update the code to this version.

Disabling lookup feature in Log4j

Disabling in configuration file (recommended)

Add the following content to the `log4j2.component.properties` configuration file (if it doesn't exist, manually create one) in `classpath` of Log4j 2.9.1 or later:

```
log4j2.formatMsgNoLookups=True
log4j.formatMsgNoLookups=True
```

Disabling through JVM parameter configuration (not recommended as the configuration can be easily lost)

Add `-Dlog4j2.formatMsgNoLookups=true` and `-Dlog4j.formatMsgNoLookups=true` to the JVM startup parameters.

©2013-2022 Tencent Cloud. All rights reserved.

Note：
For versions 2.0–2.10, you should upgrade them to 2.10 or later first and then add JVM parameters.

Upgrading JDK to later versions (recommended)

As JDK on a later version has some security limits, we recommend you upgrade JDK to 6u211, 7u201, 8u191, or 11.0.1 or later. This can block vulnerability exploit methods such as JNDI to a certain extent.

Other temporary mitigation measures

You can use a firewall or security group to prohibit relevant applications and businesses from actively connecting to the public network.

Tencent Security Solution

Tencent Cloud WAF can detect and block attacks exploiting the Log4j 2 RCE vulnerability.

References

For more information, see Apache Log4j Security Vulnerabilities.

©2013-2022 Tencent Cloud. All rights reserved.

Notice for WebLogic Console HTTP RCE Vulnerability

Last updated：2022-06-23 11:14:26

Vulnerability Details

On October 20, 2020, Tencent Security noticed that Oracle released a patch update advisory. It revealed WebLogic vulnerabilities, among which CVE-2020-14882 and CVE-2020-14883 existed in the WebLogic console, a default component on all WebLogic versions. Attackers can exploit CVE-2020-14882 and CVE-2020-14883 to execute arbitrary code on the server, obtain system permissions, and control the server without authorization, compromising data confidentiality, integrity, and availability.
All Tencent Security services have upgraded rules and vulnerability libraries accordingly to prevent attacks.
To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers.

Risk Level

High Risk

Vulnerability Risk

Attackers can exploit the vulnerabilities to control Oracle WebLogic Server, compromising data confidentiality, integrity, and availability.

Affected Versions

Oracle WebLogic Server 10.3.6.0.0
Oracle WebLogic Server 12.1.3.0.0
Oracle WebLogic Server 12.2.1.3.0
Oracle WebLogic Server 12.2.1.4.0
Oracle WebLogic Server 14.1.1.0.0

©2013-2022 Tencent Cloud. All rights reserved.

Suggestions for Fix

A new version has been officially released to fix the vulnerabilities. Tencent Security recommends you:

Recommendation solution: Install the patch in time.

Use WAF to block similar WebLogic vulnerability attacks.

References

For more information, see Oracle Critical Patch Update Advisory - October 2020.

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Exchange Server Command Execution Vulnerability

Last updated：2022-06-23 11:14:26

On September 17, 2020, Tencent Security noticed that Microsoft issued a security advisory for a command execution vulnerability in Exchange Server (CVE-2020-16875).

Note:

Microsoft Exchange Server is an email service program offered by Microsoft Corporation, which provides various features such as mail access, storage, forwarding, voice mail, and mail filtering.

The POC of the vulnerability is being circulated on the internet. Tencent Security recommends you upgrade Exchange to the latest version in time and implement asset inspection and protection to avoid attacks by hackers. Tencent Cloud WAF currently supports defense against them.

Vulnerability Details

A remote code execution vulnerability exists in Microsoft Exchange Server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user. Exploitation of the vulnerability requires successful authentication by Exchange. As the Exchange service ran with SYSTEM privileges, an attacker could get the highest privileges of the system by exploiting this vulnerability.

Affected Versions

Microsoft Exchange Server 2016 Cumulative Update 16
Microsoft Exchange Server 2016 Cumulative Update 17
Microsoft Exchange Server 2019 Cumulative Update 5
Microsoft Exchange Server 2019 Cumulative Update 6

Suggestions for Fix

According to the vulnerability advisory, Tencent Security recommends you:
Update to the latest version for fix in time.
Use WAF to detect and block attacks.

©2013-2022 Tencent Cloud. All rights reserved.

References

CVE-2020-16875

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Yonyou GRP-U8 SQL Injection Vulnerability

Last updated：2022-06-23 11:14:26

On September 11, 2020, Tencent Security noticed a SQL injection vulnerability in Yonyou GRP-U8 internal control and management software for government affairs. Attackers can use a carefully constructed payload to perform SQL injection attacks in order to get sensitive database information.
Exploitations in the wild (ITW) have been detected, and Tencent Cloud WAF supports defense against them.

Vulnerability Details

Attackers can use a carefully constructed payload to perform SQL injection attacks in order to get sensitive database information, and Tencent Cloud WAF currently supports defense against them.

Affected Versions

Yonyou GRP-U8 internal control and management software for government affairs.

Suggestions for Fix

According to the vulnerability advisory, there is currently no official update. Tencent Security recommends you:
Restrain exposing the software to the public network due to its sensitivity or use an allowlist policy.
Use WAF to detect and block attacks.

References

CNVD-2020-49261
Yonyou Gov website

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Apache Cocoon XXE Vulnerability (CVE-2020-11991)

Last updated：2022-06-23 11:14:26

On September 11, 2020, the Apache Software Foundation issued a security advisory to fix the XXE vulnerability in Apache Cocoon (CVE-2020-11991).

Vulnerability Details

Apache Cocoon is a Spring-based framework built around the concepts of separation. All processing jobs under it are linearly connected by predefined processing components, which can process the inputs and generated outputs in a pipeline sequence. Its users include Apache Lenya, Daisy CMS, Hippo CMS, Mindquarry, etc. It is usually used as a data ETL tool or relay for data transfer between systems.
CVE-2020-11991 is related to StreamGenerator. When using the StreamGenerator, Cocoon parses a user-provided XML. A specially crafted XML, including external system entities, could be used to access any file on the server system.

Risk Level

High Risk

Vulnerability Risk

A specially crafted XML, including external system entities, could be used to access any file on the server system.

Affected Versions

Apache Cocoon <= 2.1.12

Suggestions for Fix

The vulnerability has been officially fixed in the new version. Tencent Security recommends you:

©2013-2022 Tencent Cloud. All rights reserved.

Upgrade to the latest version (2.1.13) of Apache Cocoon.

Use Tencent Cloud WAF that supports detection of and defense against XXE vulnerabilities like CVE-2020-11991.

Note:

Back up your data before installing the patch to avoid accidental losses.

References

Official update notice:

Apache Cocoon

Apache Cocoon 2.2

CVE-2020-11991

©2013-2022 Tencent Cloud. All rights reserved.

Notice for WordPress File Manager Arbitrary Code Execution Vulnerability

Last updated：2022-06-23 11:14:27

On September 6, 2020, Tencent Security noticed an arbitrary code execution vulnerability in the File Manager plugin of WordPress. Attackers can exploit this vulnerability to upload trojans and run arbitrary commands and malicious scripts on WordPress websites that contain File Manager.
Tencent Security has captured exploitations in the wild (ITW), and Tencent Cloud WAF currently supports defense against them.

Vulnerability Details

Tencent Security noticed an arbitrary code execution vulnerability in the File Manager plugin of WordPress. Attackers can exploit this vulnerability to upload trojans and run arbitrary commands and malicious scripts on WordPress websites that contain File Manager. In the plugin library of wordpress.org, the version 6.8 provided by File Manager before September 1, 2020 is the affected version, which can be used by attackers to damage websites.
File lib/php/*.php can be by default opened directly, and this file loads lib/php/*.php which reads POST/GET variables, and then allows executing some internal features, like uploading files. PHP is allowed, thus this leads to unauthenticated arbitrary file upload and remote code execution.

Affected Versions

WordPress File Manager < 6.9

Suggestions for Fix

An upgraded plugin has been officially released to fix this vulnerability. Tencent Security recommends you:
Update WordPress File Manager to 6.9 or later.
Use WAF to detect and block attacks.

References

CVE 2020-25213

©2013-2022 Tencent Cloud. All rights reserved.

Jenkins Security Advisory for September

Last updated：2022-06-23 11:14:27

On September 3, 2020, Tencent Security noticed that Jenkins issued its security advisory for September, which contained 14 CVE vulnerabilities (CVE-2020-2238, CVE-2020-2239, CVE-2020-2240, CVE-2020-2241, CVE-2020-2242, CVE-2020-2243, CVE-2020-2244, CVE-2020-2245, CVE-2020-2246, CVE-2020-2247, CVE-2020-2248, CVE-2020-2249, CVE-2020-2250, and CVE-2020-2251) with 10 plugins affected, including:

Build Failure Analyzer Plugin

Cadence vManager Plugin

database Plugin

Git Parameter Plugin

JSGames Plugin

Klocwork Analysis Plugin

Parameterized Remote Trigger Plugin

SoapUI Pro Functional Testing Plugin

Team Foundation Server Plugin

Valgrind Plugin

The following vulnerabilities are defined as high for severity:

CVE-2020-2248 (XSS vulnerability in JSGames Plugin)

CVE-2020-2247 (XXE vulnerability in Klocwork Analysis Plugin)

CVE-2020-2246 (XSS vulnerability in Valgrind Plugin)

CVE-2020-2245 (XXE vulnerability in Valgrind Plugin)

CVE-2020-2244 (XSS vulnerability in Build Failure Analyzer Plugin)

CVE-2020-2243 (Stored XSS vulnerability in Cadence vManager Plugin)

CVE-2020-2240 (CSRF vulnerability in database Plugin)

CVE-2020-2238 (Stored XSS vulnerability in Git Parameter Plugin)

Jenkins is an open-source automated middleware project based on Java for continuous integration and delivery and is commonly used in the development process. To avoid impact on your business, Tencent Security recommends you conduct a security inspection in time. If your business is affected, update and fix the vulnerabilities promptly to prevent intrusions by attackers. As some vulnerabilities have no fixes yet, we recommend you use Tencent Cloud WAF for defense.

Vulnerability Details

Stored XSS vulnerability in Git Parameter Plugin (CVE-2020-2238)

©2013-2022 Tencent Cloud. All rights reserved.

Git Parameter Plugin 0.9.12 and earlier do not escape the repository field on the "Build with Parameters" page. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.
This vulnerability is fixed on Git Parameter Plugin 0.9.13.
Secret stored in plaintext by Parameterized Remote Trigger Plugin (CVE-2020-2239).
Parameterized Remote Trigger Plugin 3.1.3 and earlier store a secret in plaintext.

CSRF vulnerability in database Plugin (CVE-2020-2240)

database Plugin 1.6 and earlier do not require POST requests for the database console, resulting in a cross-site request forgery (CSRF) vulnerability. This vulnerability allows attackers to execute arbitrary SQL scripts.
CSRF vulnerability and missing permission checks in database Plugin (CVE-2020-2241 (CSRF), CVE-2020-2242 (permission check)).
database Plugin 1.6 and earlier do not perform a permission check in a method implementing form validation. This allows attackers with Overall/Read access to Jenkins to connect to an attacker-specified database server using attacker-specified username and password. Additionally, this form validation method does not require POST requests, resulting in a cross-site request forgery (CSRF) vulnerability.
database Plugin 1.7 requires POST requests and Overall/Read permission for the affected form validation method.

Stored XSS vulnerability in Cadence vManager Plugin (CVE-2020-2243)

Cadence vManager Plugin 3.0.4 and earlier do not escape build descriptions in tooltips. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission.
Cadence vManager Plugin 3.0.5 removes affected tooltips.

XSS vulnerability in Build Failure Analyzer Plugin (CVE-2020-2244)

Build Failure Analyzer Plugin 1.27.0 and earlier do not escape matching text in a form validation response. This results in a cross-site scripting (XSS) vulnerability exploitable by attackers able to provide console output for builds used to test build log indications.
Build Failure Analyzer Plugin 1.27.1 escapes matching text in the affected form validation response.

XXE vulnerability in Valgrind Plugin (CVE-2020-2245)

Valgrind Plugin 0.28 and earlier do not configure the XML parser to prevent XML external entity (XXE) attacks. This allows a user able to control the input files for the Valgrind Plugin parser to have Jenkins parse a crafted file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.
As of publication of this advisory, there is no fix.

XSS vulnerability in Valgrind Plugin (CVE-2020-2246)

Valgrind Plugin 0.28 and earlier do not escape content in Valgrind XML reports. This results in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control Valgrind XML report contents.
As of publication of this advisory, there is no fix.

XXE vulnerability in Klocwork Analysis Plugin (CVE-2020-2247)

Klocwork Analysis Plugin 2020.2.1 and earlier do not configure the XML parser to prevent XML external entity (XXE) attacks. This allows a user able to control the input files for the Klocwork plugin parser to have Jenkins parse a crafted file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.
As of publication of this advisory, there is no fix.

©2013-2022 Tencent Cloud. All rights reserved.

Reflected XSS vulnerability in JSGames Plugin (CVE-2020-2248)

JSGames Plugin 0.2 and earlier evaluate part of a URL as code. This results in a reflected cross-site scripting (XSS) vulnerability.

As of publication of this advisory, there is no fix.

Credentials stored in plaintext by Team Foundation Server Plugin (CVE-2020-2249)

Team Foundation Server Plugin 5.157.1 and earlier store a webhook secret unencrypted in the global configuration file hudson.plugins.tfs.TeamPluginGlobalConfig.xml on the Jenkins controller as part of the configuration. This secret can be viewed by attackers with access to the Jenkins controller file system.

Passwords stored in plaintext by SoapUI Pro Functional Testing Plugin (CVE-2020-2250)

SoapUI Pro Functional Testing Plugin 1.3 and earlier store project passwords unencrypted in job config.xml files as part of the configuration. These project passwords can be viewed by attackers with Extended Read permission or access to the Jenkins controller file system. SoapUI Pro Functional Testing Plugin 1.4 stores project passwords encrypted once affected job configurations are saved again.

Passwords transmitted in plaintext by SoapUI Pro Functional Testing Plugin (CVE-2020-2251)

SoapUI Pro Functional Testing Plugin stores project passwords in job config.xml files on the Jenkins controller as part of the configuration.

While these passwords are stored encrypted on disk since SoapUI Pro Functional Testing Plugin 1.4, they are transmitted in plaintext as part of the global configuration form by SoapUI Pro Functional Testing Plugin 1.5 and earlier. These passwords can be viewed by attackers with Extended Read permission.

This only affects Jenkins earlier than 2.236, including 2.235.x LTS, as Jenkins 2.236 introduces a security hardening that transparently encrypts and decrypts data used for a Jenkins password form field.

As of publication of this advisory, there is no fix.

Risk Level

CVE-2020-2249: Low

CVE-2020-2239: Low

CVE-2020-2241: Medium

CVE-2020-2242: Medium

CVE-2020-2250: Medium

CVE-2020-2251: Medium

CVE-2020-2240: High

CVE-2020-2247: High

CVE-2020-2248: High

CVE-2020-2246: High

CVE-2020-2245: High

CVE-2020-2243: High

©2013-2022 Tencent Cloud. All rights reserved.

CVE-2020-2238: High

CVE-2020-2244: High

Affected Versions

Build Failure Analyzer Plugin <= 1.27.0

Cadence vManager Plugin <= 3.0.4

database Plugin <= 1.6

Git Parameter Plugin <= 0.9.12

JSGames Plugin <= 0.2

Klocwork Analysis Plugin <= 2020.2.1

Parameterized Remote Trigger Plugin <= 3.1.3

SoapUI Pro Functional Testing Plugin <= 1.3

SoapUI Pro Functional Testing Plugin <= 1.5

Team Foundation Server Plugin <= 5.157.1

Valgrind Plugin <= 0.28

Fixed Versions

Build Failure Analyzer Plugin should be updated to version 1.27.1

Cadence vManager Plugin should be updated to version 3.0.5

database Plugin should be updated to version 1.7

Git Parameter Plugin should be updated to version 0.9.13

Parameterized Remote Trigger Plugin should be updated to version 3.1.4

SoapUI Pro Functional Testing Plugin should be updated to version 1.4

Versions to Be Fixed

JSGames Plugin

Klocwork Analysis Plugin

SoapUI Pro Functional Testing Plugin

Team Foundation Server Plugin

Valgrind Plugin

Suggestions for Fix

©2013-2022 Tencent Cloud. All rights reserved.

Certain upgraded plugins have been officially released to fix these vulnerabilities; however, as some of them have no fix yet, Tencent Security recommends you:

Update the corresponding Jenkins plugins (as the plaintext storage vulnerability is a local vulnerability, you need to wait for the plugin update).

Restrain exposing Jenkins to the public network due to its sensitivity. If there is a need for public network access, you can configure an access policy such as IP allowlist in WAF.

Use WAF to detect and block network-based attacks through the vulnerabilities in the Jenkins Security Advisory for September.

WAF supports detection of and defense against all the vulnerabilities contained in the Jenkins Security Advisory for September.

References

The official advisories are as follows:

Jenkins Security Advisory 2020-09-01

CVE-2020-2238

CVE-2020-2239

CVE-2020-2240

CVE-2020-2241

CVE-2020-2242

CVE-2020-2243

CVE-2020-2244

CVE-2020-2245

CVE-2020-2246

CVE-2020-2247

CVE-2020-2248

CVE-2020-2249

CVE-2020-2250

CVE-2020-2251

XSS vulnerability in CloudBees Jenkins (CVE-2020-2246)

XSS vulnerability in CloudBees Jenkins (CVE-2020-2243)

XXE vulnerability in CloudBees Jenkins

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Apache Struts 2 RCE Vulnerabilities (CVE-2019-0230 and CVE-2019-0233)

Last updated：2022-06-23 11:14:27

On August 13, 2020, Tencent Security noticed that Apache Struts issued a security advisory for the S2-059 Struts remote code execution vulnerability and S2-060 Struts denial of service vulnerability.

Vulnerability Details

Apache Struts 2 is a web framework for developing Java EE network applications.
S2-059 Struts remote code execution vulnerability (CVE-2019-0230): In cases such as improper use of certain tags, OGNL expression injection may exist, thereby causing a remote code execution vulnerability.
S2-060 Struts denial of service vulnerability (CVE-2019-0233): It may cause denial of service attacks when files are uploaded and manipulated.

Affected Versions

Apache Struts 2.0.0–2.5.20

Safe Versions

Apache Struts >= 2.5.22

Suggestions for Fix

Based on the vulnerability information, Tencent Security recommends you:
Upgrade the Apache Struts framework to the latest version.
Use Tencent Cloud WAF, an AI-based one-stop web security solution. The most typical characteristic of the S2-059 vulnerability is that it uses the OGNL language. The Tencent Security technical team conducted a targeted study on OGNL expressions, blocked attacks against such expressions, and integrated the defense capability into WAF. Therefore, as long as the vulnerability is attacked based on OGNL expressions, WAF can directly block them.
In addition, the intelligent engine of WAF also provides intelligent defense against SQL, XSS, and command execution

©2013-2022 Tencent Cloud. All rights reserved.

attacks. Backed by AI technologies, it can reasonably and effectively block unknown security vulnerabilities for improved business continuity.

References

Official advisory:

CVE-2019-0230

CVE-2019-0233

©2013-2022 Tencent Cloud. All rights reserved.

Notice for Apache SkyWalking SQL Injection Vulnerability (CVE-2020-13921)

Last updated：2022-06-23 11:14:27

On August 5, 2020, Tencent Force (force.tencent.com) researched and noticed that Apache SkyWalking had a SQL injection vulnerability (CVE-2020-13921). A new version has been officially released to fix this vulnerability.
To safeguard your business, we recommend you conduct a security inspection in time. If your business is affected, update it to fix the vulnerability promptly and prevent intrusions by attackers. For more information, see Affected Versions.

Vulnerability Details

Apache SkyWalking is an application performance monitor (APM) tool that provides automated and high-performance monitoring solutions for microservices, cloud native, and container-based applications. Its official website shows that it is being used by a large number of Chinese companies in the internet, banking, and civil aviation sectors.
In multiple versions of SkyWalking, unauthorized GraphQL APIs are opened by default, through which attackers can construct malicious request packets for SQL injection, resulting in the leakage of sensitive information in the user database. In view of the greater impact of this vulnerability, we recommend you fix it as soon as possible.

Risk Level

High Risk

Vulnerability Risk

Through SQL injection, attackers can steal sensitive information on servers.

Affected Versions

Apache SkyWalking 6.0.0–6.6.0
Apache SkyWalking 7.0.0
Apache SkyWalking 8.0.0–8.0.1

©2013-2022 Tencent Cloud. All rights reserved.

Fix

Apache SkyWalking 8.1.0

Suggestions for Fix

A new version has been officially released to fix this vulnerability. Tencent Security recommends you:
Recommended solution: Upgrade to Apache SkyWalking 8.1.0 or later.
Temporary mitigation: If the upgrade is temporarily impossible, as a mitigation measure, we recommend you restrain exposing the GraphQL APIs of Apache SkyWalking to the public network or add a layer of authentication on top of such APIs.
-**Recommendation for organizational users**: Use Tencent Security services to detect and block attacks through this Apache SkyWalking SQL injection vulnerability.
Tencent Cloud WAF supports detection of and defense against attacks through this SkyWalking SQL injection vulnerability.

References

If needed, you can find more information of the vulnerability here.

©2013-2022 Tencent Cloud. All rights reserved.