Web Application Firewall

Security Advisory

Product Documentation

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

Security Advisory
- Command Execution Vulnerability in Exchange Server
- SQL Injection Vulnerability in Yonyou GRP-U8
- XXE Vulnerability in Apache Cocoon (CVE-2020-11991)
- Arbitrary Code Execution Vulnerability in WordPress File Manager
- Jenkins Security Advisory for September
- Remote Code Execution Vulnerabilities in Apache Struts 2 (CVE-2019-0230 and CVE-2019-0233)
- SQL Injection Vulnerability in Apache SkyWalking (CVE-2020-13921)

Security Advisory
Command Execution Vulnerability in Exchange Server

Last updated : 2020-12-15 15:20:26

On September 17, 2020, Tencent Security detected 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.

References

CVE-2020-16875

SQL Injection Vulnerability in Yonyou GRP-U8

Last updated : 2020-12-15 15:20:27

On September 11, 2020, Tencent Security detected an 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

XXE Vulnerability in Apache Cocoon (CVE-2020-11991)

Last updated : 2020-12-15 15:20:27

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.

Severity

High

Risks

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:

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

Arbitrary Code Execution Vulnerability in WordPress File Manager

Last updated : 2020-12-15 15:20:27

On September 6, 2020, Tencent Security detected 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 detected 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 v6.9 and above.
- Use WAF to detect and block attacks.

References

CVE 2020-25213

Jenkins Security Advisory for September

Last updated : 2021-01-06 11:04:39

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, please 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)**
    - Git Parameter Plugin 0.9.12 and earlier does 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 plain text by Parameterized Remote Trigger Plugin (CVE-2020-2239).
    - Parameterized Remote Trigger Plugin 3.1.3 and earlier stores a secret in plain text.

- **CSRF vulnerability in database Plugin (CVE-2020-2240)**
    - database Plugin 1.6 and earlier does 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 does 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 does 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 does 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 om Valgrind Plugin (CVE-2020-2245)**
  - Valgrind Plugin 0.28 and earlier does not configure its 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 does 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.

- **XE vulnerability in Klocwork Analysis Plugin (CVE-2020-2247)**
  - Klocwork Analysis Plugin 2020.2.1 and earlier does not configure its 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.

- **Reflected XSS vulnerability in JSGames Plugin (CVE-2020-2248)**
  - JSGames Plugin 0.2 and earlier evaluates 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 plain text by Team Foundation Server Plugin (CVE-2020-2249)**
  Team Foundation Server Plugin 5.157.1 and earlier stores a webhook secret unencrypted in its global configuration file hudson.plugins.tfs.TeamPluginGlobalConfig.xml on the Jenkins controller as part of its configuration. This secret can be viewed by attackers with access to the Jenkins controller file system.

- **Passwords stored in plain text by SoapUI Pro Functional Testing Plugin (CVE-2020-2250)**
  SoapUI Pro Functional Testing Plugin 1.3 and earlier stores project passwords unencrypted in job config.xml files as part of its 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 plain text 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 its configuration.
  - While these passwords are stored encrypted on disk since SoapUI Pro Functional Testing Plugin 1.4, they are transmitted in plain text 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 before 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.

Severity

- 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
- 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

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 plain text 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 advisory is 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

Remote Code Execution Vulnerabilities in Apache Struts 2 (CVE-2019-0230 and CVE-2019-0233)

Last updated : 2020-12-15 15:20:27

On August 13, 2020, Tencent Security detected 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

Secure 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 the vulnerability 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 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

SQL Injection Vulnerability in Apache SkyWalking (CVE-2020-13921)

Last updated : 2020-12-15 15:20:27

On August 5, 2020, Tencent Force (force.tencent.com) researched and discovered that Apache SkyWalking had a SQL injection vulnerability (CVE-2020-13921). A new version has been officially released to fix this vulnerability.

To avoid impact on your business, Tencent Security recommends you conduct a security inspection in time. If your business is affected, please update and fix the vulnerabilities promptly to prevent intrusions by attackers. For more information, please 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.

Severity

High

Risks

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

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 above.
- **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.