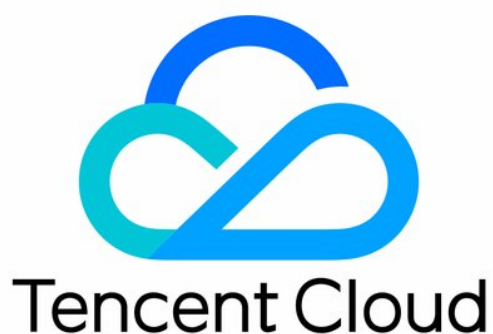


Cloud Workload Protection Platform Practical Tutorial



Copyright Notice

©2013–2025 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice



This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Practical Tutorial

Interpretation Of Host Security Classified Protection Assessment

Auto Fix Of Vulnerabilities

Scan Code Login Security

Malicious File Handling

Practical Tutorial

Interpretation Of Host Security

Classified Protection Assessment

Last updated: 2025-02-27 11:26:17

Interpretation Of Classified Protection Standard

Tencent Cloud Workload Protection (CWPP) product complies with the main standards of the level protection 2.0 system. According to the "[Basic Requirements for Cybersecurity Level Protection](#)" (GB/T 22239-2019), Tencent CWPP (limited to the Professional and Ultimate editions with purchased log analysis) meets the security requirements of level three and below:

No	Classified Protection Standard Section	Classified Protection Standard Serial Number	Classified Protection Standard Content	Corresponding Feature Description
1	Security area boundary—Boundary Protection	8.1.3.1 c)	It should be able to check and limit unauthorized connections from internal users to the public network.	CWPP supports detecting and intercepting unauthorized malicious outbound connections from Cloud Virtual Machines to external malicious domain names and IP addresses.
2	Security boundary – Intrusion prevention	8.1.3.3 a)	It should detect, prevent, or limit network attacks initiated from outside at key network nodes.	CWPP supports detecting and blocking brute force attacks, detecting common network attacks, and one-click vulnerability defense for some vulnerabilities.

3	Security boundary – Intrusion prevention	8.1.3.3 b)	Network attacks initiated from inside should be detected, prevented, or limited at key network nodes.	CWPP can detect outbound connections and attack behaviors at the system layer and application layer of CVM, and send alarms for abnormal process and command behaviors.
4	Security boundary – Intrusion prevention	8.1.3.3 c)	Technical measures should be taken to analyze network behaviors, achieving analysis of network attacks, especially new types of network attacks.	CWPP supports analysis based on security data from hosts, networks, and cloud platforms, enabling detection and alarms for new attacks such as mining, ransomware, Trojans, and worms.
5	Security boundary – Intrusion prevention	8.1.3.3 d)	When an attack is detected, record the source IP, attack type, attack purpose, and attack time. An alarm should be provided in the event of a serious intrusion event.	When CWPP detects a brute force attack, it records the source IP, source location, attacked server IP/name, port, protocol, username, time, cracking status, blocking status, and sends an alarm.
6	Security boundary – Security audit	8.1.3.5 b)	Audit records should include the date and time of the event, user, event type, whether the event was successful, and other audit-related information.	CWPP supports server login audit, recording information including source IP, source location, server IP/name, login username, login time, status, and risk level.
7	Secure computing environment –	8.1.4.1 a)	Users logging in should be identified and authenticated. Identifiers should be	CWPP baseline check capability supports regular security checks on cloud

	Identity authentication		unique, and authentication information should meet complexity requirements and be periodically replaced.	service customer login configurations and password complexity, provides warnings for risk items, and offers security advice.
8	Secure computing environment – Identity authentication	8.1.4.1 b)	The login failure processing feature should be enabled, and measures such as ending session, limiting the number of unauthorized login attempts, and automatically exiting when the login connection times out should be configured and enabled.	CWPP supports host login failure defense configuration, allowing flexible configuration of rules to lock users after multiple login failures within a certain time period.
9	Secure computing environment – Identity authentication	8.1.4.1 c)	Necessary measures should be taken to prevent authentication info from being eavesdropped during network transmission when performing remote management.	CWPP supports checks for improper remote management configurations, such as a baseline check prohibiting the use of telnet.
10	Secure computing environment – Access control	8.1.4.2 b)	The default account should be renamed or deleted, and the default password of the default account should be modified.	CWPP supports account permission configuration checks. Asset management supports displaying all login accounts, supports default weak password security checks, and provides alarms and remediation suggestions when risks are detected.

1 1	Secure computing environment – Access control	8.1.4.2 c)	Redundant or expired accounts should be deleted or disabled in a timely manner to avoid the existence of shared accounts.	CWPP supports security configuration checks for CVM accounts. Asset management supports displaying all login accounts, provides alarms for abnormal account login IPs, and supports alerts to avoid the existence of shared accounts.
1 2	Secure computing environment – Security audit	8.1.4.3 a)	Security audit should be enabled, covering each user, auditing important user behaviors and significant security events.	CWPP supports recording cloud server account login operations, as well as auditing high-risk commands and high-risk operations.
1 3	Secure computing environment – Security audit	8.1.4.3 b)	Audit records should include the date and time of the event, user, event type, whether the event was successful, and other audit-related information.	CWPP log records include host IP, host instance ID, account, source IP, destination IP, process ID, port, event type, occurrence time, action policy, etc.
1 4	Secure computing environment – Security audit	8.1.4.3 c)	Audit records should be protected, regularly backed up, and prevented from unexpected deletion, modification, or overwrite.	The host security product supports a log audit storage feature, which can store log data for at least 6 months. Different tenants use completely independent log spaces, and log data has a multi-replica backup mechanism.

1 5	Secure computing environment – Intrusion prevention	8.1.4.4 b)	Unnecessary system services, Default Sharing, and high-risk ports should be closed.	CWPP asset management supports unified control of services, processes, and open ports running on cloud servers.
1 6	Secure computing environment – Intrusion prevention	8.1.4.4 c)	Management terminals accessed via the network should be restricted by setting terminal access methods or network address ranges.	CWPP supports adding allowlists for host login IP addresses. Logins from non-allowlisted users will be blocked. Combined with security groups, it enables cloud network management and restriction.
1 7	Secure computing environment – Intrusion prevention	8.1.4.4 e)	It should be able to detect potential known vulnerabilities and fix them promptly after thorough testing and evaluation.	CWPP supports detecting Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities, and emergency vulnerabilities, assessing risk levels, and providing remediation suggestions.
1 8	Secure computing environment – Intrusion prevention	8.1.4.4 f)	It should be able to detect intrusions on critical nodes and provide alarms when serious intrusion events occur.	CWPP supports detecting intrusions on critical nodes, including malicious files, abnormal logins, password cracking, malicious requests, high-risk commands, rebound shell, local privilege escalation,

				file tampering, and other threats, providing alarms and some proactive blocking capabilities.
19	Secure computing environment – Malicious code prevention	8.1.4.5	Technical measures to prevent malicious code attacks or proactive immune verify trustworthiness mechanisms should be used to promptly identify and effectively block intrusions and viruses.	CWPP supports malicious file scanning and killing, real-time monitoring of Trojans, viruses, and automatic isolation.
20	Security Management Center – Security Management	8.1.5.3 a)	Security administrators should undergo identity authentication, be allowed to perform security management operations only through specific commands or operation interfaces, and these operations should be audited.	CWPP supports security management operations on cloud resources through the console, and can audit login behaviors and high-risk commands.
21	Security Management Center – Security Management	8.1.5.3 b)	Security policies in the system should be configured by security administrators, including setting security parameters, uniformly marking Subjects and objects, authorizing Subjects, and configuring trusted verification policies.	CWPP supports configuring security policies in the host system through the console.
22	Security Management Center –	8.1.5.3 e)	Centralized management should be conducted for	CWPP supports centralized management of

	Centralized Control		security policies, malicious code, patch upgrades, and other security-related matters.	vulnerabilities, malicious code detection, and isolation for host security.
--	---------------------	--	--	---

Cybersecurity Classified Protection Compliance Service Baseline Policy

Tencent Cloud CWPP by default provides the [Cybersecurity Classified Protection Compliance Baseline Policy](#), supporting periodic detection and one-click detection of baseline detection items. It helps understand the baseline pass rate and risk situation, provides risk levels and remediation suggestions for baselines and detection items, aiding in quick rectification to meet compliance requirements. The following are the supported detection items for Cybersecurity Classified Protection Compliance:

Baseline Categorization	Baseline Name	Number Of Included Check Items
Classified Protection Level 2	Level-2 Cybersecurity Classified Protection – CentOS 6 Security Baseline Check	16
	Level-2 Cybersecurity Classified Protection – CentOS 7 Security Baseline Check	18
	Level-2 Cybersecurity Classified Protection – CentOS 8 Security Baseline Check	16
	Level-2 Cybersecurity Classified Protection – Ubuntu 14 Security Baseline Check	19
	Level-2 Cybersecurity Classified Protection – Ubuntu 16 Security Baseline Check	19
	Level-2 Cybersecurity Classified Protection – Ubuntu 18 Security Baseline Check	21
	Level-2 Cybersecurity Classified Protection – Ubuntu 20 Security Baseline Check	29
Classified Protection Level 3	Level-3 Cybersecurity Classified Protection – CentOS 6 Security Baseline Check	27
	Level-3 Cybersecurity Classified Protection –	31

	CentOS 7 Security Baseline Check	
	Level-3 Cybersecurity Classified Protection – CentOS 8 Security Baseline Check	36
	Level-3 Cybersecurity Classified Protection – Ubuntu 14 Security Baseline Check	35
	Level-3 Cybersecurity Classified Protection – Ubuntu 16 Security Baseline Check	33
	Level-3 Cybersecurity Classified Protection – Ubuntu 18 Security Baseline Check	40
	Level-3 Cybersecurity Classified Protection – Ubuntu 20 Security Baseline Check	48
	Level-3 Cybersecurity Classified Protection – Windows 2008 Security Baseline Check	19
	Level-3 Cybersecurity Classified Protection – Windows 2012 Security Baseline Check	19
	Level-3 Cybersecurity Classified Protection – Windows 2016 Security Baseline Check	19

Auto Fix Of Vulnerabilities

Last updated: 2025-02-27 11:28:48

This topic describes the tutorial for automatically fixing vulnerabilities.

Note:

Auto-fixing of vulnerabilities may involve executing commands on your servers, which may affect running applications or core system components, and may impact your business continuity. For servers used for your core business, we recommend that you take the impact into full consideration when deciding which vulnerabilities to fix and in what order.

Explanation

- Supported servers: Only CVM servers on Tencent Cloud (host security client online and bound with CWPP Ultimate license).
- Vulnerabilities that can be fixed automatically: Linux software vulnerabilities (some) and Web-CMS vulnerabilities (some).

Operation Guide

1. Log in to the [CWPP Console](#) and click **Vulnerability Management** in the left navigation pane. Then the list of detected vulnerabilities is shown at the bottom.
2. The **Vulnerability List** is categorized into Emergency Vulnerabilities and All Vulnerabilities. Since both are displayed from the detection dimension, there is not much difference in functionality. The steps for fixing vulnerabilities automatically are described below using **All Vulnerabilities** as an example.

Note:

- Vulnerability Fix Priorities: Urgent vulnerabilities > High-priority vulnerabilities > All vulnerabilities.
- For vulnerabilities that can be automatically fixed, **Auto Fix** is shown in the operation column; for vulnerabilities that cannot be automatically fixed, **Fix Scheme** is shown in the column.

应急漏洞

全部漏洞

显示统计图表

自动修复

更多处理

全部漏洞标签

高危, 严重

待修复

仅展示高优修复漏洞 判定规则

请输入漏洞名称/CVE编号搜索

<input type="checkbox"/>	漏洞名称/标签	检测方式	漏洞类型	威胁等级	全网攻击热度	CV...	CVE编号	最后扫描...	影响...	处理状态	自动修复状态	操作
<input type="checkbox"/>	Adiscon Rsyslog 缓冲... 远程利用 存在POC	版本对比	Linux软...	严重	<div></div> <div></div> <div></div>	9.8	CVE-201...	2023-06-08 11:27:58	1	待修复	可自动修复(无需重启)	自动修复 更多
<input type="checkbox"/>	Adiscon Rsyslog 缓冲... 远程利用	版本对比	Linux软...	严重	<div></div> <div></div> <div></div>	9.8	CVE-201...	2023-06-08 11:27:58	1	待修复	可自动修复(无需重启)	自动修复 更多
<input type="checkbox"/>	Python 输入验证错误... 远程利用	版本对比	Linux软...	高危	<div></div> <div></div> <div></div>	7.5	CVE-201...	2023-06-08 11:27:58	1	待修复	可自动修复(无需重启)	自动修复 更多
<input type="checkbox"/>	Bash 输入验证错误漏... 本地利用	版本对比	Linux软...	高危	<div></div> <div></div> <div></div>	7.8	CVE-201...	2023-06-08 11:27:58	1	待修复	可自动修复(无需重启)	自动修复 更多
<input type="checkbox"/>	Apache Solr ConfigSe... 远程利用 存在POC	版本对比	应用漏洞	严重	<div></div> <div></div> <div></div>	9.8	CVE-202...	2023-06-08 11:27:58	1	待修复	暂不支持修复	修复方案 更多

Step 1: View Vulnerability Details

Click **Auto Fix** to open the vulnerability details pop-up window.

PostgreSQL JDBC远程代码执行漏洞(CVE-2022-21724) CVSS评分 9.8漏洞详情 [导出](#)

漏洞名称 PostgreSQL JDBC远程代码执行漏洞(CVE-2022-21724)

漏洞标签 远程利用

漏洞类型 应用漏洞

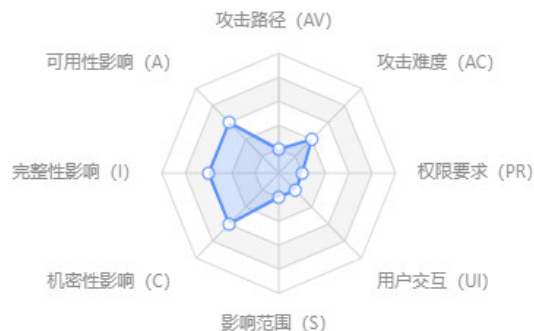
威胁等级 严重

CVE编号 CVE-2022-21724

披露时间 2022-02-02

漏洞描述 PostgreSQL JDBC Driver是一个用 Pure Java (Type 4) 编写的开源 JDBC 驱动程序，用于 PostgreSQL 本地网络协议中进行通信。

PostgreSQL JDBC Driver (简称 PgJDBC) 存在安全漏洞，该漏洞源于pgjdbc连接属性提供的类名实例化插件实例，驱动程序在实例化类之前并不验证类是否实现了预期的接口从而导致远程代码。



修复方案

修复方案 建议受影响的用户及时更新pgjdbc到安全版本；

42.2.x及之前版本，请升级到42.2.25或42.3.2及以上版本；

42.3.x用户请升级到42.3.2及以上版本；

下载链接：

<https://jdbc.postgresql.org/download/>

扫描到服务器存在漏洞风险，建议立即对相关主机进行快照备份，避免遭受损失。

参考链接 <https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-v7wg-cpwc-24m4>

<https://github.com/pgjdbc/pgjdbc/commit/f4d0ed69c0b3aae8531d83d6af4c57f22312c813>

<https://security.netapp.com/advisory/ntap-20220311-0005/>

[更多2条参考链接](#)

影响主机范围 (1)

修复	重新扫描	忽略	待修复	请选择资源属性后输入关键字进行过滤(仅支持单个值)				Q	刷新	下载
<input type="checkbox"/>	主机名称/实...	IP地址	防护版本	服务器状态	扫描时间	说明	状态	操作		
<input type="checkbox"/>	172.17.0.1	172.17.0.1	旗舰版	运行中	首次: 2022-02-02 最近: 2022-02-02	漏洞详情	待修复	重新扫描 忽略漏洞		

Step 2: Select the Host To Fix

1. In the list of affected servers, select the host you want to fix and click **Fix**.



2. In the confirmation pop-up, click **Confirm** to enter the vulnerability fix page.

Step 3: Choose Whether To Create Snapshots

1. On the vulnerability modification page, confirm the range of hosts to be fixed and click **Next**.
2. Choose the repair method based on actual needs:
 - **Fix and Automatically Create Snapshots:** You can set the snapshot name and snapshot storage duration (3 days, 7 days, or 15 days). It is recommended to set the duration to 7 days so that the snapshots can be rolled back in time if necessary.
 - **Fix Without Creating Snapshots:** If snapshots have been created for all the servers selected for fixing vulnerabilities on the current day, this item becomes optional.

[← 修复漏洞：Git 代码执行漏洞\(CVE-2023-29007\)](#)* 关闭抽屉后点击“修复详情”按钮方可再次查看流程 [×](#)

① 修复说明

② 选择修复方式

③ 创建快照&修复漏洞

漏洞修复说明

- 修复可能持续10~20分钟，具体时长与服务器当前工作情况相关，请耐心等待；
- 此漏洞执行修复后需重启方可修复成功，建议您根据业务情况谨慎选择修复时间；
- 主机进行漏洞补丁修复行为可能存在一定风险，为了防止出现业务中断或异常，建议您先通过 控制台手动创建快照 并 自行搭建环境充分测试修复方案，具体操作请参考 [主机漏洞修复指南](#) [🔗](#)

☒ 自动创建快照并修复☐ 不创建快照直接修复

快照名称

漏洞修复_Git 代码执行漏洞(CVE-2023-29007)

[?](#)

快照保存时长

7天 (建议)

▼

1. 创建快照建议保留7天时间，以便在有需求的情况下及时回滚。

2. 创建快照需要额外的费用 (500GB/天约2元)，详细计费可见 [快照价格总览](#) [🔗](#)

Step 4: Fix Vulnerabilities

Click **Confirm** to start fixing the vulnerabilities. You can keep track of the process.

← 修复漏洞: Git 代码执行漏洞(CVE-2023-29007)

* 关闭抽屉后点击“修复详情”按钮方可再次查看流程 X

修复说明

选择修复方式

3 创建快照&修复漏洞



全部修复成功

返回

已修复主机/目标主机2 / 2

开始时间2023-06-09 15:43:09

结束时间2023-06-09 15:44:47

创建快照

收起

服务器IP/名称	快照名称	创建状态	快照创建时间
1[redacted]	漏洞修复_Git 代码执行漏洞(CVE-202...	创建成功	2023-06-09 15:43:47
1[redacted]	漏洞修复_Git 代码执行漏洞(CVE-202...	创建成功	2023-06-09 15:43:57

修复漏洞: Git 代码执行漏洞(CVE-2023-29007)

收起

服务器IP/名称	修复状态	修复时间
1[redacted] (手动)	修复成功	2023-06-09 15:44:33
1[redacted]	修复成功	2023-06-09 15:44:47

修复完成

Step 5: Check the Server Status Changes

Return to **Vulnerability Details** and monitor the host status changes. If the vulnerability fix fails, the status will be fix failure; if the vulnerability fix succeeds, the status will change to fixed.

Git 代码执行漏洞(CVE-2023-29007)

CVSS评分

7.8

X

漏洞描述 Git是一套免费、开源的分布式版本控制系统。Git存在注入漏洞。攻击者利用该漏洞可以远程执行代码。

影响范围 (5)

修复方案

修复方案 建议您更新当前系统或软件至最新版，完成漏洞的修复。
扫描到服务器存在漏洞风险，建议立即对相关主机进行快照备份，避免遭受损失。

参考链接 <https://github.com/git/git/security/advisories/GHSA-v48j-4xgg-4844>
<https://github.com/git/git/commit/528290f8c61222433a8cf02fb7cffa8438432b4>
<https://github.com/git/git/blob/9ce9dea4e1c2419cca126d29fa7730baa078a11b/Documentation/RelNotes/2.30.9.txt>
[更多3条参考连接](#)

影响主机范围 (10)

影响组件范围 (4)

修复	重新扫描	忽略	全部	请选择资源属性后输入关键字进行过滤(仅支持单个值)				Q	↺	↓
<input type="checkbox"/>	主机名称/实...	IP地址	防护版本	服务器状态	扫描时间	说明	状态	操作		
<input type="checkbox"/>	暂无标签	公 内	旗舰版	运行中	首次: 2023-05-23 17:42:42 最近: 2023-06-09 15:44:47	-	已修复	回滚 重新扫描 修复详情		
<input type="checkbox"/>	暂无标签	公 内	旗舰版	运行中	首次: 2023-05-16 01:39:23 最近: 2023-06-09 15:44:32	-	已修复	回滚 重新扫描 修复详情		

- After the vulnerabilities are fixed, if your business is greatly affected, click **Rollback** to go to **CVM > Snapshot List**, and select the snapshots created before the fixing to roll back. After the rollback is successful, restart the servers to scan the vulnerabilities again.
- After the vulnerabilities are fixed, perform a **Rescan** to verify whether the vulnerabilities have been fixed.
- After the vulnerabilities are fixed, you can also click **Repair details** to view the specific repair process.

Scan Code Login Security

Last updated: 2025-02-27 11:29:19

The secure login feature via QR code scanning allows users to log in to the server by simply verifying through WeChat QR code scanning without entering a password. This feature effectively prevents brute force attacks by hackers, thereby enhancing server security and increasing login convenience. This article will introduce a practical tutorial on secure login via QR code scanning.

Note:

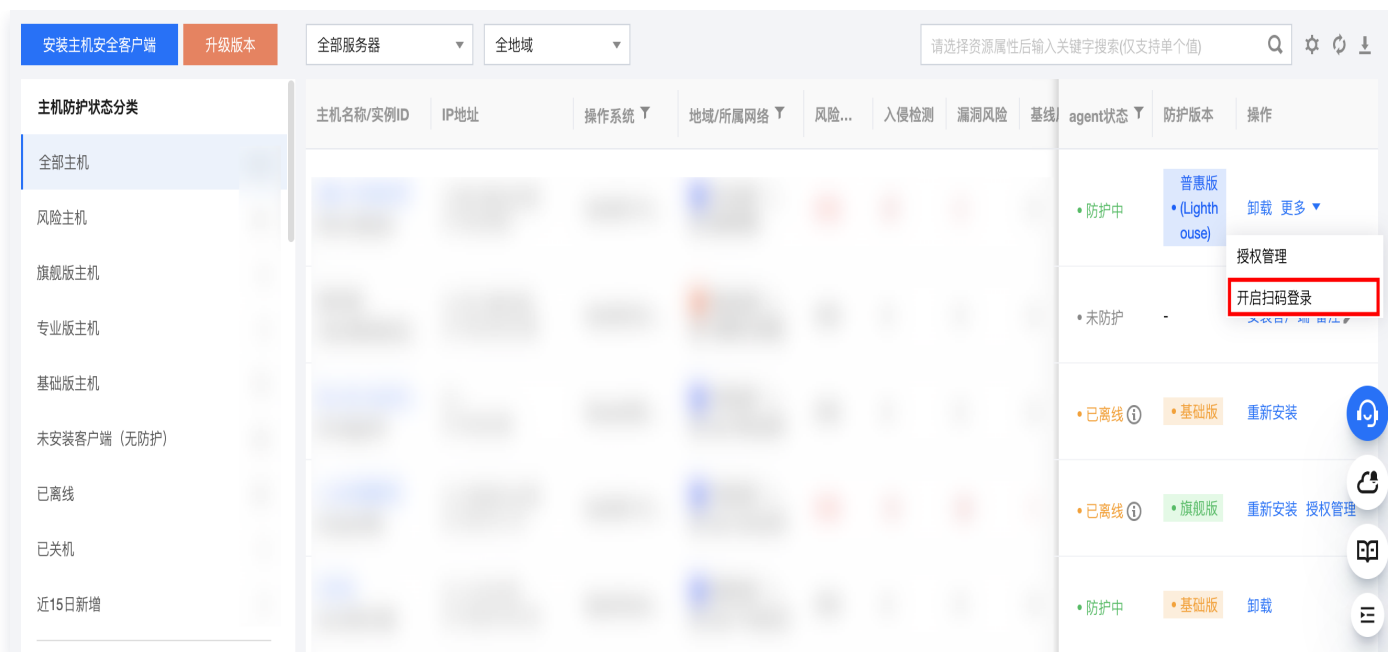
- After enabling QR code login, WeChat QR code verification will replace password login for Tencent Cloud account, which may affect related automated business. Meanwhile, when using SSH-related protocols, although SCP, SFTP, RSYNC, GIT, MOSH, and other scenarios are supported, scenarios like folder mounting based on SSHFS protocol are not yet supported.
- **For hosts of core business, it is recommended to fully consider before deciding whether to change the login method.**

Explanation

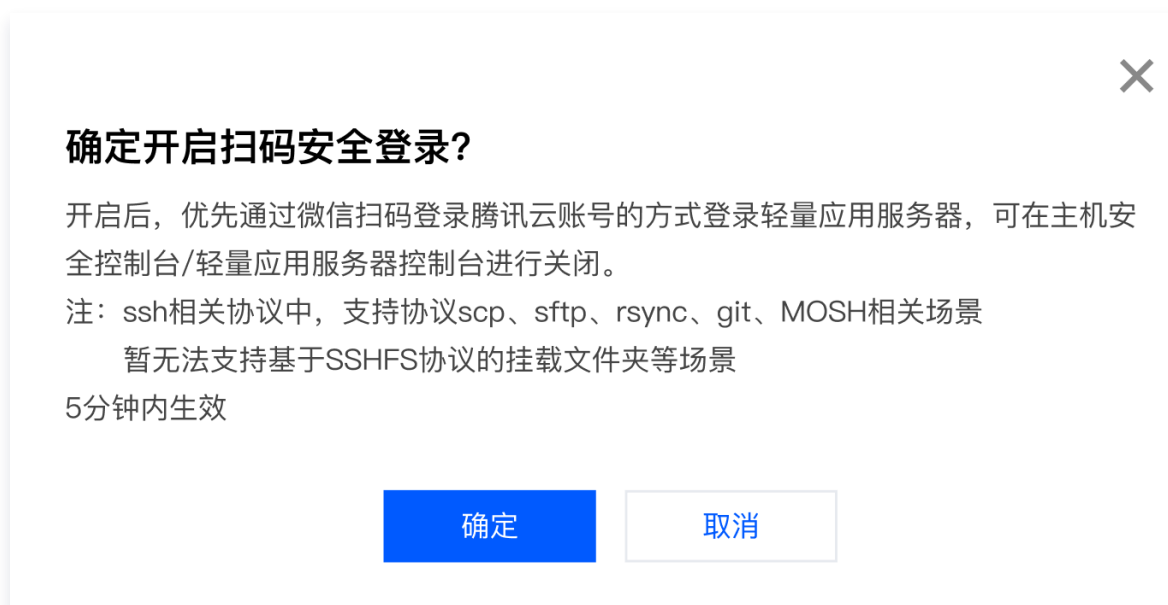
- Supported host types: Only CVM/Lighthouse servers on Tencent Cloud (requires Cloud Workload Protection Platform client to be online).
- Supported login users: The Tencent Cloud sub-account and its root account to which the machine belongs, or other Tencent Cloud accounts authorized by CAM.

Step 1: Configure the Login Method

1. Log in to the [CWPP Console](#), and in the left navigation bar, click **Host List**.
2. In the host list, find the corresponding instance on the right side, and click **Enable QR Code Login**.



3. Click **Confirm**. After enabling, the server will preferentially log in through a Tencent Cloud account by scanning the QR code with WeChat.



Step 2: Terminal Initiates Login

1. After enabling QR code login, a QR code will pop up after entering the instance IP in the SSH command line. Use WeChat to scan the code to enter the Tencent Cloud Assistant mini program for identity authentication. After completing the authentication, you can log in.

ⓘ Note:

If there is an issue with the QR code display, please open the QR code image in a web page using the URL provided below.

```
almainhan@ALMAINHAN-MB0 ~ %
almainhan@ALMAINHAN-MB0 ~ % ssh root@11
```



```
*****
If the QR code cannot be displayed normally, it is recommended to execute
Visit the URL: https://s          >g
*****
```

2. When the QR code login service encounters an exception, it will automatically downgrade to the standard password login, and a captcha fallback strategy will be added. After entering the random number to complete the authentication, you can log in using the password.

```
almainhan@ALMAINHAN-MB0 ~ %
almainhan@ALMAINHAN-MB0 ~ % ssh root@11
```

```
*****
There is a service failure when logging in by scanning the QR code. We have switched your login method to password login.
*****
For security reasons, please enter the verification code 2077 to complete the verification:2077
root@11 's password: ?
```

Step 3: Mini Program Verification

1. After scanning the code, open Tencent Cloud Assistant, select the login method to log in to the Tencent Cloud account to complete the verification.



没有账号? [立即注册](#)

登录腾讯云



微信登录

上次登录



邮箱登录



我已阅读并同意 [腾讯云服务协议](#)、[腾讯云隐私声明](#)
和 [腾讯云账号协议](#)

其他登录方式



QQ



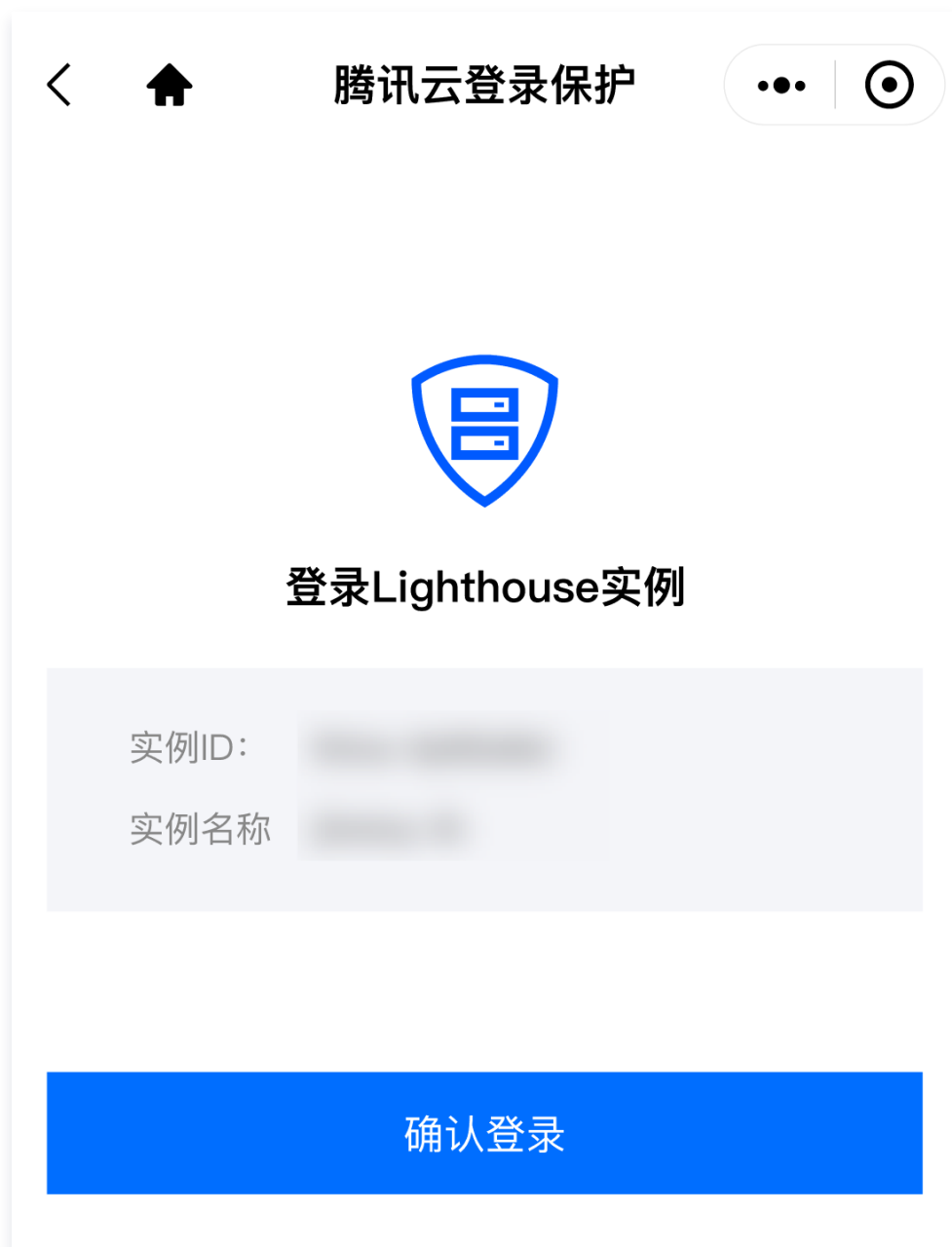
子用户

[忘记账号](#) | [忘记密码](#) | [登录异常帮助文档](#)

Copyright © 2013 – 2024 Tencent Cloud.

All Right Reserved. 腾讯云 版权所有

2. Successfully log in to the Tencent Cloud account, click **Confirm Login**, verify the account's permission to log in to the server, and complete the login after verification.



Malicious File Handling

Last updated: 2025-02-27 11:52:37

When a server under a user's Tencent Cloud account is detected with a malicious file, if Host Security finds that the file is not in the allowlist, a real-time alarm will be triggered.

Processing Procedures

After receiving a malicious file alert, follow these steps:

1. Log in to the [CWPP Console](#), and select **Intrusion Detection > Malicious File Scan** from the left sidebar.
2. On the Malicious File Scan page, search by **Alarm Asset ID** to locate the specific alarm and click **Details**.

The screenshot shows the Tencent Cloud CWPP Console interface. The left sidebar contains navigation options such as '主机安全' (Host Security), '安全概览' (Security Overview), '资产中心' (Asset Center), '资产概览' (Asset Overview), '主机列表' (Host List), '资产指纹' (Asset Fingerprint), '安全预警' (Security Alert), '安全加固' (Security Reinforcement), '漏洞管理' (Vulnerability Management), '基线管理' (Baseline Management), '入侵防御' (Intrusion Prevention), '入侵检测' (Intrusion Detection), '文件查杀' (File Scanning), '异常登录' (Abnormal Login), '密码破解' (Password Cracking), '恶意请求' (Malicious Request), '高危命令' (High-risk Command), '本地提权' (Local Privilege Escalation), '反弹Shell' (Reverse Shell), '高级防御' (Advanced Defense), '安全运营' (Security Operations), and '日志分析' (Log Analysis). The main content area is titled '文件查杀' (File Scanning) and includes a '告警列表' (Alert List) tab. Below the tab, there is a '功能使用说明' (Feature Usage Guide) section with four steps: 1. Upgrade professional/flagship edition, 2. File scanning settings/download manual scan, 3. Obtain alerts, and 4. Alert processing. A '风险概况' (Risk Overview) section shows the current status of the system, including the number of hosts at risk (3), the number of hosts with pending alerts (0), and the number of hosts with pending alerts (1). A '开始扫描' (Start Scan) button is available. Below the risk overview, there is a table of detected malicious files. The table has columns for '主机名称/实例ID' (Host Name/Instance ID), 'IP地址' (IP Address), '路径' (Path), '病毒名/检出引擎' (Virus Name/Detection Engine), '威胁等级' (Threat Level), '首次发现时间' (First Discovery Time), '最近检测时间' (Last Detection Time), '处理状态' (Processing Status), and '操作' (Action). The table lists three detected files: 'Script.Trojan.Exec.Jcniw', 'Suspicious.aiScore=m', and 'Linux.HackTool.Lsh.Aplw'. The 'Script.Trojan.Exec.Jcniw' file is highlighted with a red box, and the 'Details' button in the '操作' column is also highlighted with a red box.

3. After viewing the alarm details, confirm whether the malicious file is a false alarm. If it is a false alarm, proceed to step 4. If it is not a false alarm, proceed to step 5.

Note:

Whether the malicious file is a false alarm can be determined by the following methods:

- Contact the business team to determine if the file is necessary for normal business operations.
- Query threat intelligence to determine if the file is marked as a malicious sample by the public network.
- Determine if the file's behavior triggers more alarms.
- Contact [Security Expert Service](#).

4. If it is confirmed as a false alarm, add the file to the allowlist. Future detections of this file will be ignored and will not trigger an alarm. Contact us for [Feedback on False Alarms](#).

添加白名单

白名单内容

* 加白方式

☒ 文件MD5 ☐ 自定义文件

* 文件MD5

请输入文件MD5，多个回车换行，一行输入一个MD5
示例：
19a7ae0aea306b7165b3431c90f613b2
7cbfd6268396ad16e1880e6d3f2e2f2e

告警处理

☒ 对符合本规则的历史“待处理”告警执行加白操作

生效主机范围（已选择 3 台）

选择范围

☒ 全部专业版和旗舰版服务器 ☐ 自选服务器

5. If it is confirmed not to be a false alarm, follow the remediation suggestions in the alarm details to handle it.

恶意文件详情 待处理

隔离标记已处理加入白名单忽略删除记录

告警详情

进程树 NEW事件调查 NEW

风险主机



主机名称

实例 ID

公

内

• 客户端在线

首次发现时间 2024-09-03 10:22:56

最近检测时间 2024-10-21 02:18:42

病毒文件



病毒名

威胁等级 严重

检出引擎

标签特征 Exploit



文件名

文件大小 1.50 KB

文件路径

文件MD5

最近访问时间 2024-10-20 12:33:55

最近修改时间 2024-09-03 10:22:39

危害描述

告警描述

发现主机/容器上存在漏洞利用程序，您的主机/容器可能已经失陷。
漏洞利用程序是指黑客针对某些特定的程序漏洞编写的攻击程序，黑客可能借此入侵您的系统。

修复建议

建议方案

1.隔离或者删除相关的木马文件；
2.对系统进行风险排查，并进行安全加固，详情可参考如下链接：
【Linux】<https://cloud.tencent.com/document/product/296/9604>
【Windows】<https://cloud.tencent.com/document/product/296/9605>

参考链接

暂无

- You can click **Isolation** to isolate the file and terminate the related process. The Alarm processing status will change to "Isolated".
- You can log in to the host, find the corresponding file, manually delete or isolate it and terminate the related process, then mark the Alarm as processed in the console. The Alarm processing status will change to "Processed".

6. On the Malicious File Scan page, click **Scan Settings** in the upper right corner. It is recommended to enable the automatic isolation switch to automatically isolate detected malicious files immediately.

©2013–2025 Tencent Cloud. All rights reserved.

Page 27 of 30

查杀设置



专业版/旗舰版主机均支持定时检测和实时监控，自动隔离功能属于旗舰版功能，建议您 [升级版本](#) 启用更多安全防护功能。

定时扫描

实时监控 NEW**自动隔离**

规则内容

自动隔离

☒ 开启或关闭自动隔离，均需要进行配置，实际生效存在几分钟延迟，请知悉。

主机安全将自动隔离检测出的恶意文件，部分恶意文件仍需用户手动确认隔离，建议您检查文件查杀中的告警列表，确保已全部处理。若出现误隔离，请在已隔离列表中对文件进行恢复。

杀掉进程：☒ 杀掉该文件相关进程，建议勾选

防护模式

标准模式

重保模式

仅针对高置信度的风险进行自动防护，更适合日常安全运营使用。 推荐

Note:

- Not all detected malicious files can be automatically isolated. Some malicious files still require manual confirmation for isolation. It is recommended to check the alarm list in file scanning to ensure all have been handled.
- If a false positive isolation occurs, please restore the file from the isolated list.
- Enabling or disabling automatic isolation requires configuration, and there is a delay of a few minutes before it takes effect.

Hot Issues

Where To Configure Alarms For Malicious Files?

On the [Alarm Settings](#) page, configure the alarm time, alarm scope, and alarm items for **Malicious File Scan – Malicious File**.

主机安全

漏洞管理

基线管理

入侵防御

入侵检测

文件查杀

异常登录

密码破解

恶意请求

高危命令

本地提权

反弹Shell

高级防护

安全运营

日志分析

专家服务

设置中心

授权管理

告警设置

其他应用

云立体防护

主机安全容器版

给产品打个分

告警设置

站内信/短信/邮件等

机器人通知

重要声明

产生待处理告警时，主机安全系统会根据配置的告警规则向指定的用户发送告警通知。告警设置包括如下步骤：

请确认消息订阅中“主机安全”消息设置了接收模式、接收渠道和接收人（特别说明：主机安全暂不支持语音告警，即使接收渠道中勾选了“语音”也不会发送语音告警）前往设置

配置主机安全各类事件是否告警、告警时间及告警项。

告警时间：默认全天24小时，可自定义（告警周期开始时，前3条安全事件实时告警，后续每2小时汇总告警1次）

告警项：具体告警内容或告警事件威胁等级（支持勾选）。

入侵检测

告警类型	告警状态	告警时间	告警主机范围	告警项
文件查杀-恶意文件	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	<input checked="" type="checkbox"/> 严重 <input checked="" type="checkbox"/> 高危 <input type="checkbox"/> 中危 <input type="checkbox"/> 低危 <input type="checkbox"/> 提示
文件查杀-异常进程	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	检测到内存中存在正在运行的异常进程
异常登录	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	<input checked="" type="checkbox"/> 高危 <input checked="" type="checkbox"/> 可疑
密码破解	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	登录密码被破解成功
恶意请求	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	服务器请求了恶意域名
高危命令	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	<input checked="" type="checkbox"/> 高危 <input type="checkbox"/> 中危 <input type="checkbox"/> 低危
本地提权	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	系统中出现低权限试图提高权限
反弹Shell	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	服务器上出现Shell反向连接
网页防篡改	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> 全天 <input type="text" value="09:00"/> ~ <input type="text" value="18:00"/>	全部主机 编辑	<input checked="" type="checkbox"/> 篡改成功 <input checked="" type="checkbox"/> 恢复失败

How To Set Up Periodic Detection For Malicious Files?

On the [Malicious File Scan page](#), click **Scan Settings** in the upper right corner to open the scan settings popup and set up a scheduled scan.

查杀设置

专业版/旗舰版主机均支持定时检测和实时监控，自动隔离功能属于旗舰版功能，建议您 [升级版本](#) 启用更多安全防护功能。

定时扫描

实时监控

NEW

自动隔离

开启定时扫描



定期扫描主机木马病毒文件，增强安全性

检测模式 ⓘ

全盘检测 ▼

除快速检测范围外，会检测系统所有分区

异常进程检测



深度检测内存中的异常进程，可能造成一定程度的资源占用率升高，请谨慎选择。

检测周期

每隔3天 ▼

02:00 ~ 06:00



检测范围

检测范围



全部专业版和旗舰版服务器



自选服务器

If the File Has Been Deleted, What Will Be the Status Of the Original Alarm After Scanning For Malicious Files Again?

The original alarm processing status will change to "Cleared."