

Cloud Workload Protection Platform

Practical Tutorial

Product Documentation



Copyright Notice

©2013–2026 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



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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

Practical Tutorial

Auto Fix of Vulnerabilities

Malicious File Processing

Practical Tutorial

Auto Fix of Vulnerabilities

Last updated: 2026-01-22 14:20:11

This topic describes the best practices 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 restarting applications or operating systems, which may affect your business continuity. For servers that are used for your core business, we recommend that you take the impact into full consideration when planning which vulnerabilities to fix and in what order to do so.

Limitations

Servers that support fixing:

- Tencent Cloud servers and non-Tencent Cloud servers (with the CWPP client online and bound to a CWPP Ultimate Edition license)
- The automatic snapshot creation feature is only supported for Tencent Cloud CVM and Lighthouse servers. Other types of servers do not currently support automatic snapshot creation. For these servers, you can create a backup manually and then select "Directly fix without creating snapshots" during the process to perform vulnerability fixing.

Vulnerabilities that support fixing:

- Linux software vulnerabilities (partial)
- Web-CMS vulnerabilities (partial)

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 vulnerabilities in the **Vulnerability List** are categorized as Urgent Vulnerabilities, Critical Vulnerabilities, and All Vulnerabilities, which are discovered vulnerabilities that are not obviously different from each other in terms of functionality. The steps for fixing vulnerabilities automatically are described below using **All Vulnerabilities** as an example.

Note:

- Priorities: Urgent vulnerabilities > Critical 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.

<input type="checkbox"/>	Vulnerability name/tag	Severity level	CVSS	CVE No.	Last scanned #	Affected... #	Processing...	Operation
<input type="checkbox"/>	PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)	Fatal	9.8	CVE-2016-5703	2022-08-30 18:01:52	1	To be fixed	Auto fix Re-scan Ignore
<input type="checkbox"/>	PhpMyAdmin dbase extension remote code execution vulnerability (CVE-...)	High	8.1	CVE-2016-6633	2022-08-30 18:01:52	1	To be fixed	Solution Re-scan Ignore
<input type="checkbox"/>	PhpMyAdmin Export function SQL injection vulnerability (CVE-2016-6617)	High	8.1	CVE-2016-6617	2022-08-30 18:01:52	1	To be fixed	Solution Re-scan Ignore

Step 1: View vulnerability details

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

PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)
CVSS score 9.8
✕

Vulnerability details

Vulnerability name: PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)

Vulnerability tag: -

Vulnerability type: Web-CMS vulnerabilities

Severity level: Fatal

CVE No.: CVE-2016-5703

Disclosure time: 2016-06-23

Vulnerability description: There is a SQL injection vulnerability in central_columns.lib.php, which can be used by hackers to attack the database and steal data, which brings harm to the data security of the server.

Solution

Solution: 1. It is recommended to upgrade to the latest official version, the official website address: <https://www.phpmyadmin.net>
Vulnerabilities detected. Please create snapshots for the servers for security reasons.

Reference: <https://www.phpmyadmin.net/security/PMASA-2016-19/>

Affected servers

Fix
Re-scan
Ignore
To be fixed ▾
Please select a tag ▾

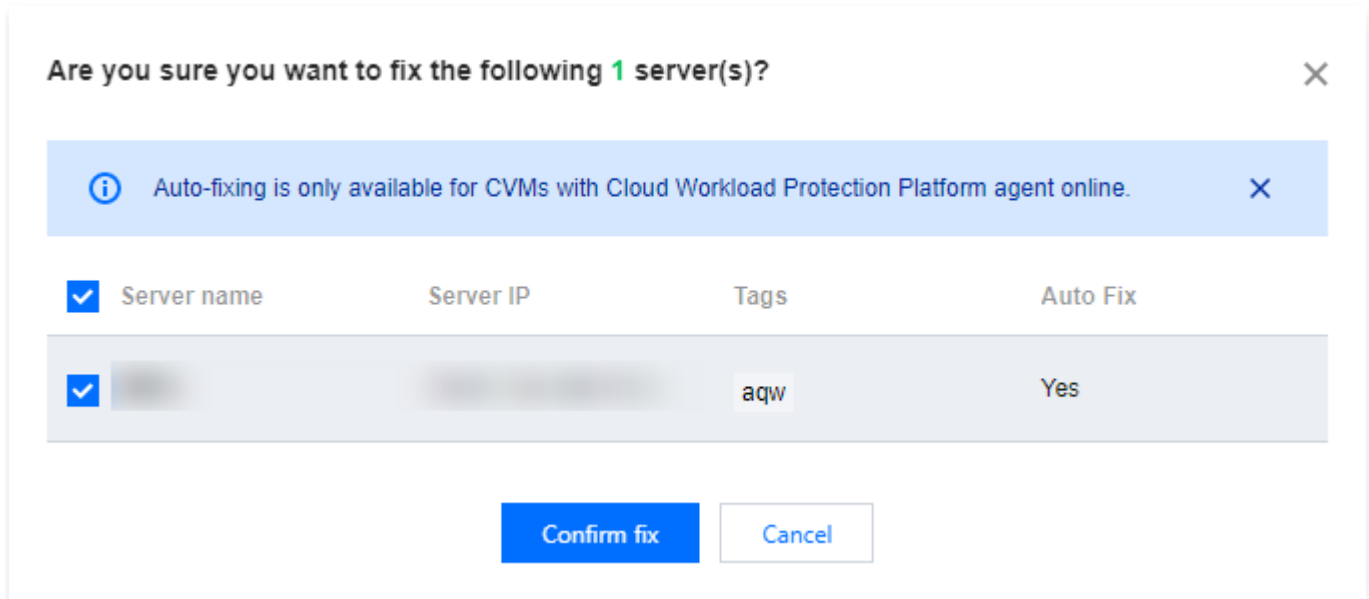
Search by server name/IP

🔍
🔄
⬇️

<input type="checkbox"/>	Server IP/Name	Ve... ▾	Server tag	Serve... ▾	Description	First dete...	Last scan...	Status	Operation
<input type="checkbox"/>	[blurred]	CWPP...	aqw	Running	There is a...	2022-08-01 11:28:43	2022-08-30 18:01:52	⊖ To be fixed	Fix Re-scan Ignore

Step 2: Select the servers for which you want to fix vulnerabilities automatically.

Select the target servers in the affected server list, and click **Fix** to open the confirmation pop-up window.



Step 3: Choose whether to create snapshots

Click **Confirm** to open the fix method configuration pop-up window, and select the fix method: Fix and Automatically Create Snapshots, or Fix Without Creating Snapshots

Fix Vulnerabilities: PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)
✕

! Fixing Description
✕

- The fix process involves snapshot creation, vulnerability fix, and re-detection.
- Creating a snapshot incurs a fee
- The fix process may take 5 minutes or more, depending on the servers.

Fixed servers (1)

Server IP/Name	Latest snapshot name	Latest snapshot name
[blurred]	-	-

Fix Method

Automatically create a snapshot and fix

Snapshot name ⓘ

Snapshot retention period Keep snapshots for 7 days so as to roll them back instantly when needed.


Directly fix without creating snapshots

- 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.

Step 4: Fix vulnerabilities

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

← Fix Vulnerabilities: PhpMyAdmin SQL inje...
✕



Fixing vulnerabilities.....

99 %

Estimated remaining time 9 sec

Fixed/Target server 0 / 1

Start time 2022-09-01 14:30:28

End time

✔ Create snapshot
▼ Collapse

Server IP/Name	Snapshot name	Creation status	Snapshot creation time
[REDACTED]	Vulnerability Fix_PhpMyAdmin SQL i...	✔ Created successfully	2022-09-01 14:31:39

🔄 Fixed vulnerabilities: PhpMyAdmin SQL injection vulnerability (C...
99%
▼ Collapse

Server IP/Name	Fix status	Fix Time
[REDACTED]	🔄 Fixing...	--

✔ Fixing completed

Step 5: Check the server status changes

Return to **Vulnerability Details** to check the server status changes. If vulnerability fixing fails, the status is "Fixing Failed"; if vulnerability fixing is successful, the status changes to "Fixed".

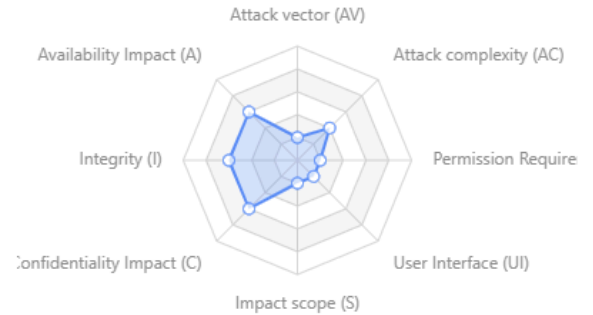
PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)

CVSS score 9.8



Vulnerability details

Vulnerability name	PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)
Vulnerability tag	-
Vulnerability type	Web-CMS vulnerabilities
Severity level	Fatal
CVE No.	CVE-2016-5703
Disclosure time	2016-06-23
Vulnerability description	There is a SQL injection vulnerability in central_columns.lib.php, which can be used by hackers to attack the database and steal data, which brings harm to the data security of the server.



Solution

Solution 1. It is recommended to upgrade to the latest official version, the official website address: <https://www.phpmyadmin.net>
Vulnerabilities detected. Please create snapshots for the servers for security reasons.

Reference <https://www.phpmyadmin.net/security/PMSA-2016-19/>

Affected servers

Fix	Re-scan	Ignore	All ▾	Please select a tag ▾	Search by server name/IP <input type="text"/>						
<input type="checkbox"/> Server IP/Name	Ve... ▾	Server tag	Serve... ▾	Description	First date...	Last scan...	Status	Operation			
<input type="checkbox"/>	CWPP...	aqw	Running	There is a...	2022-08-01 11:28:43	2022-08-30 18:01:52	Fixed	Rollback Rescan Fix Details			
Total items: 1						10 ▾ / page					

- After the vulnerabilities are fixed, if your business is greatly affected, click **Rollback** to go to [CVMs](#) > **Snapshot List**, and then select the snapshots created before the fixing to roll back them. 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.
- You can also click "Fix Details" to view the details of fixing.

Malicious File Processing

Last updated: 2025-10-29 14:44:00

When malicious files are detected on the server under a user's Tencent Cloud account, if the file is not hit in the file allowlist, real-time alerts will be triggered by host security.

Processing Steps

Upon receiving a malicious file Alarm, please follow the steps below:

1. Log in to the [CWPP Console](#). In the left sidebar, select **Intrusion Detection > Virus Scanning**.
2. On the virus scanning page, search by **Instance ID**, locate the specific alarm and click **details**.

The screenshot shows the 'Virus Scanning' interface in the Tencent Cloud console. It includes a sidebar with navigation options, a main dashboard with a 'Risk overview' section, and a table of detected malicious files. The 'Risk overview' section shows 29 malicious files pending processing, 2 unresolved abnormal processes, and 5 affected servers. The table below lists detected files with columns for Server Name/Instance ID, IP Address, Path, Virus name/Detection engine, Risk Level, First detected, Last checked, Processing Status, and Operation. A search bar is visible at the top right of the table.

Server Name/Instance ID	IP Address	Path	Virus name/Detection engine	Risk Level	First detected	Last checked	Processing Status	Operation
[Redacted]	[Redacted]	/tmp/tpu8KGF (deleted)	Linux.Trojan.Poqinfect.Osmw	Total	2024-10-24 20:26:16	2024-10-31 00:00:15	pending resolved	Details Process
[Redacted]	[Redacted]	/tmp/Z5w8P53l (deleted)	Linux.Risk.Bitcoinminer.Tdli	Total	2024-10-28 00:00:22	2024-10-31 00:00:14	pending resolved	Details Process
[Redacted]	[Redacted]	/tmp/82xL2Za7 (deleted)	Linux.Risk.Bitcoinminer.Tdli	Total	2024-10-27 00:00:10	2024-10-27 00:00:10	pending resolved	Details Process
[Redacted]	[Redacted]	/tmp/47E82DgP8 (deleted)	Linux.Risk.Bitcoinminer.Tdli	Total	2024-10-26 00:00:22	2024-10-26 00:00:22	pending resolved	Details Process
[Redacted]	[Redacted]	/tmp/47E82DgP8	Linux.Risk.Bitcoinminer.Tdli	Total	2024-10-25 21:52:26	2024-10-25 21:52:26	pending resolved	Details Process
[Redacted]	[Redacted]	/tmp/QskMwaxC35W	Linux.Risk.Bitcoinminer.Tdli	Total	2024-10-25 03:22:59	2024-10-25 03:22:59	pending resolved	Details Process
[Redacted]	[Redacted]	/tmp/P84kocvE1f (deleted)	Linux.Risk.Bitcoinminer.Tdli	Total	2024-10-24 20:26:16	2024-10-24 20:26:16	pending resolved	Details Process

3. After checking alarm details, please confirm whether this malicious file is a false alarm. If it is a false alarm, please perform step 4. If it is not a false alarm, please perform step 5.

Note:

Whether this malicious file is a false alarm can be determined by several ways.

- Contact the business team to judge whether the file is a required file for normal business operation.
- Query threat intelligence and judge whether the file is marked as a malicious sample by the public network.
- Whether this file behavior causes further triggering of more Alarms.
- Contact [Security Expert Service \(SES\)](#).

4. Clearly a false alarm. Please add this file to the allowlist. Subsequently, if this file is detected again, it will be ignored and no alarm will be generated. And [contact us](#) to report the false alarm.

Add Allowlist ✕

Allowlist

* Whitelisting Method MD5 File Custom File

* MD5 File

Please enter the file MD5, multiple return line breaks, enter one MD5 per line
Example:
19a7ae0aea306b7165b3431c90f613b2
7cbfd6268396ad16e1880e6d3f2e2f2e

Alert handling Perform whitelisting operations on historical 'pending' alerts that meet this rule

Effective host range (selected 1 server(s))

Select * All CWPP Pro and CWPP Ultimate hosts Specified servers

How to specify

Select a region

Server tag

Select host [Select all](#) **1 server(s) selected** [Clear](#)

5. Clearly not a false alarm. Please refer to the recovery suggestions in the alarm details for handling.

Malicious file details ⊖ Pending resolved ?

✕

Quarantine
Mark as processed
Add to allowlist
Ignore
Delete Log

Alarm details
Process tree
Event investigation NEW

Servers in Risks

<div style="display: flex; align-items: center; margin-bottom: 5px;"> <div style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">☰</div> <div> <p>Server name [REDACTED]</p> <p>Instance ID [REDACTED]</p> </div> </div>	<div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> ● First detected 2024-10-24 20:26:16 </div> <div style="display: flex; justify-content: space-between;"> ● Last checked 2024-10-31 00:00:15 </div>
--	--

Virus file

<div style="display: flex; align-items: center; margin-bottom: 5px;"> <div style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">⚠</div> <div> <p>Virus Name [REDACTED]</p> </div> </div>	<div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> Risk Level Fatal </div> <div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> Engine </div> <div style="display: flex; justify-content: space-between;"> Tag Characteristics - </div>
<div style="display: flex; align-items: center; margin-bottom: 5px;"> <div style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-right: 10px;">📄</div> <div> <p>File Name [REDACTED]</p> </div> </div>	<div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> File Size [REDACTED] </div> <div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> File path [REDACTED] </div> <div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> MD5 File [REDACTED] </div> <div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> Last accessed 2024-10-30 00:03:18 </div> <div style="display: flex; justify-content: space-between;"> Last modified time 2024-08-23 04:40:20 </div>

⚠ Hazard Description

Alert description It is found that there is a malicious Trojan horse on the host, and your host may have been compromised. Malicious Trojans usually perform malicious actions such as mining, file deletion, information theft, and network attacks.

🛡 How to fix

Suggestion

1. Check malicious processes and illegal ports, delete suspicious startup items and scheduled tasks;
2. Isolate or delete related Trojan files;
3. Check the risk of the system and perform security reinforcement. For details, please refer to the following link: [REDACTED]

Reference Unavailable

- – Click **Quarantine** to quarantine this file and end related processes. The alarm handling status will become "**Quarantined**".
 - – Log in to the host, find the corresponding file, manually delete or quarantine it and end related processes. Then mark the alarm as processed on the console. The alarm handling status will become "**Resolved**".
6. On the virus scanning page, click **Detection Settings** in the upper right corner. It is recommended to enable the auto-isolation switch. If a malicious file is detected, it will be automatically isolate immediately.

Detection settings

Both CWPP Pro and CWPP Ultimate support scheduled check and real-time monitoring. Auto Isolation is only available in CWPP Ultimate. Please [upgrade the edition](#) for more security features.

Scheduled Scan Real-Time Monitoring **Auto isolation**

Rule Content

Auto isolation Please note that it takes several minutes for the enabling or disabling of Auto Isolation to take effect.

The host security will automatically isolate malicious files detected, but some malicious files still require manual confirmation for isolation. It is recommended to check the alarm list in file scanning and ensure that all files have been processed. If there are any false isolations, you can restore the files from the isolated list.

Kill Process: Kill related processes of this file, recommended to select

Protection Mode **Standard** Enhanced Protection Mode

Automatically protects against high-confidence risks, more suitable for daily security operations. **Recommended**

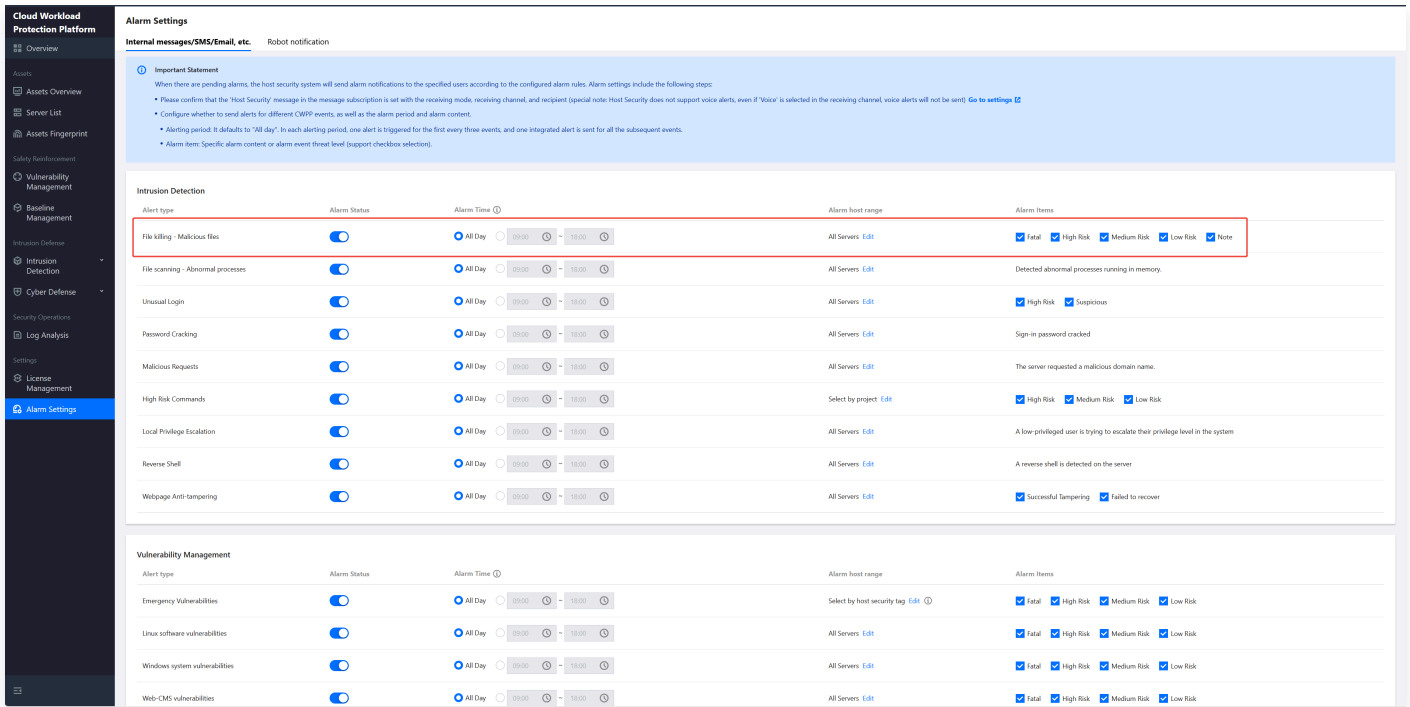
Note:

- Not all detected malicious files can be automatically quarantined. Manual confirmation of quarantine for some malicious files is still required. It is recommended to check the alarm list in the file detection and elimination and ensure all resolved.
- If a file is falsely quarantined, please restore it from the quarantined list.
- To turn on or off auto isolation, configuration is required. There is several minutes delay before taking effect.

FAQs

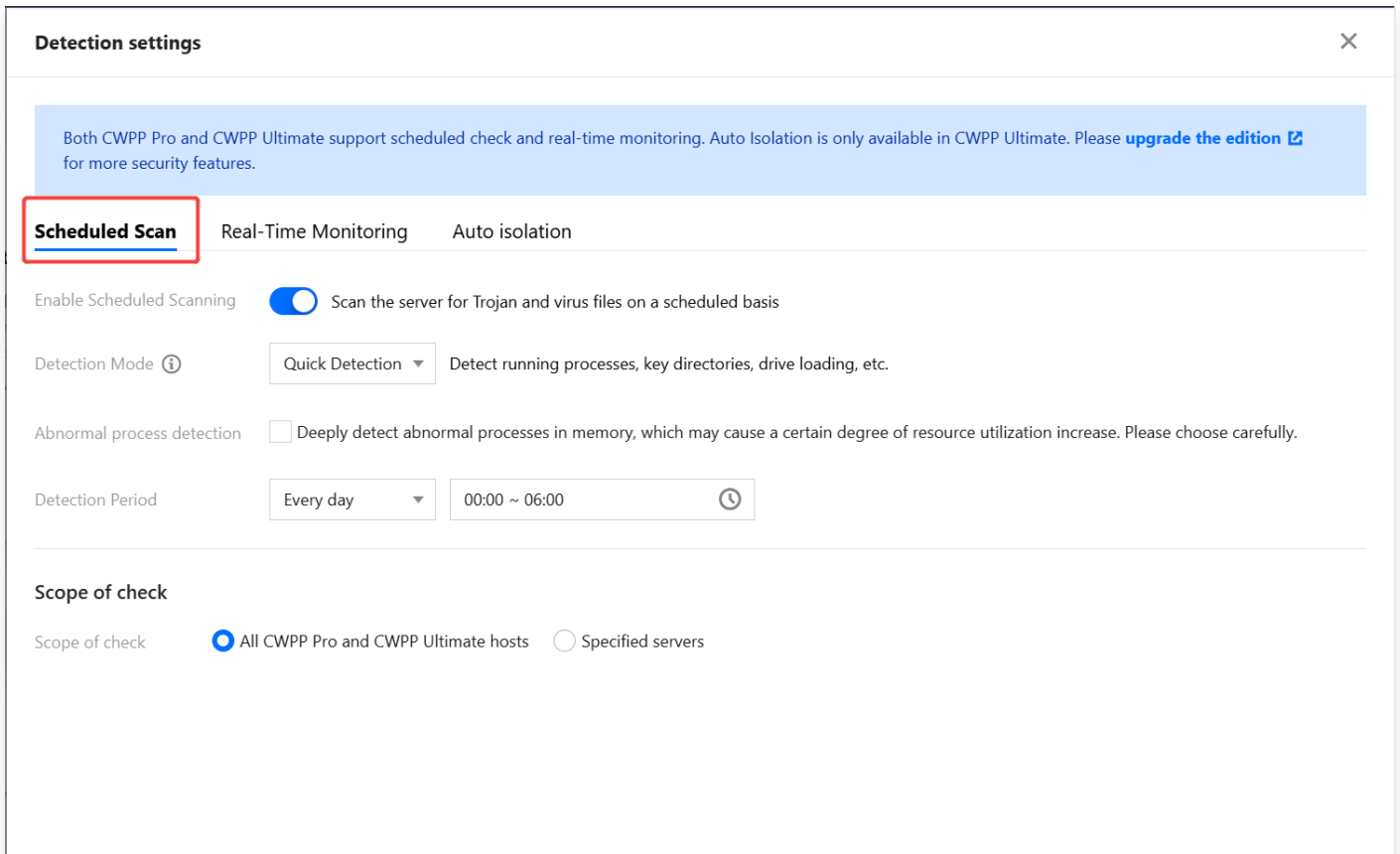
Where to Configure Alarms for Malicious Files?

On the [Alarm Settings Page](#), configure the alarm time, alarm host range, and alarm items for **file killing – malicious files**.



How to Set Up Regular Inspection for Malicious Files?

On the [virus scanning Page](#), click **Detection Settings** in the upper right corner. Open the **Detection Settings** popup and perform scheduled scan settings.



If a File Has Been Deleted and a Malicious File Scan Is Performed Again, What Will the Original Alarm Handling Status Become?

The original alarm handling status will become "cleaned".