Cloud Workload Protection Platform

Best Practices

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

Best Practices

Auto Fix of Vulnerabilities

Last updated：2023-12-26 16:39:51

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

Supported servers: CVM Ultimate on which CWPP is online.

Supported vulnerabilities: Linux software vulnerabilities (some) and Web-CMS vulnerabilities (some).

Operation Guide

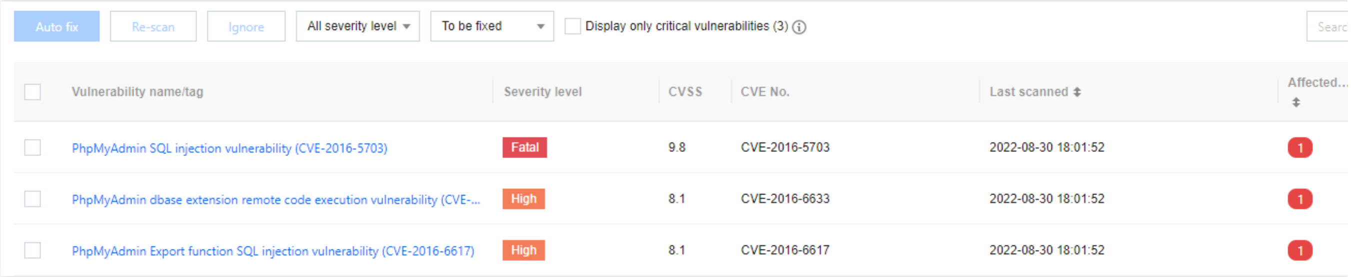
1. Log in to the CWPP Console and click **Vulnerability Management** in the left navigation pane. Then the list of detected vulnerabilities is shown at the bottom.

2. The 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.

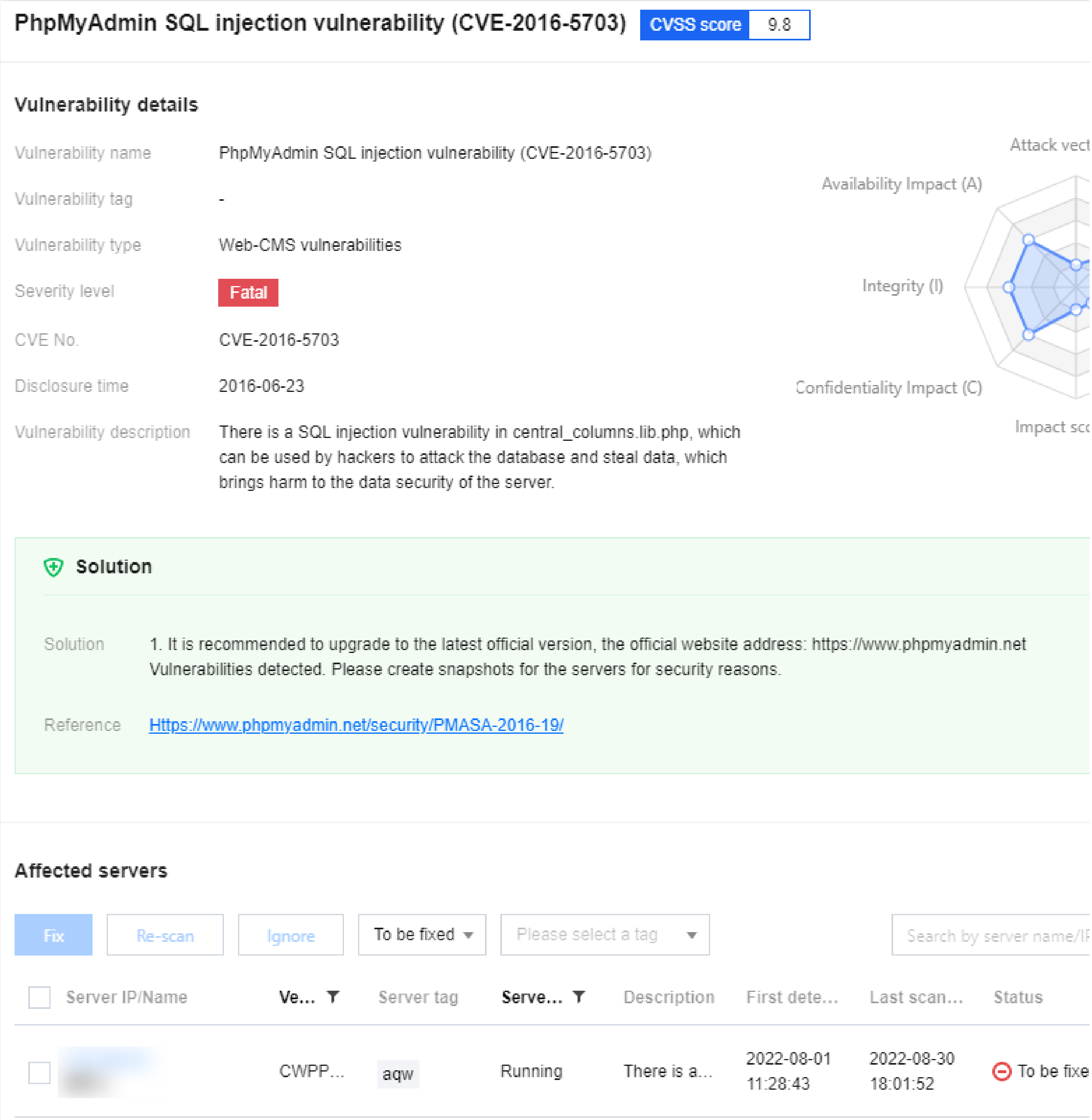
For vulnerabilities that can be automatically fixed, **Auto Fix** is shown in the operation column; for vulnerabilities that cannot be automatically fixed, **Fix Scheme** is shown in the column.



□	Vulnerability name/tag	Severity level	CVSS	CVE No.	Last scanned	Affected...
□	PhpMyAdmin SQL injection vulnerability (CVE-2016-5703)	Fatal	9.8	CVE-2016-5703	2022-08-30 18:01:52	1
□	PhpMyAdmin dbase extension remote code execution vulnerability (CVE-...	High	8.1	CVE-2016-6633	2022-08-30 18:01:52	1
□	PhpMyAdmin Export function SQL injection vulnerability (CVE-2016-6617)	High	8.1	CVE-2016-6617	2022-08-30 18:01:52	1

Step 1: View vulnerability details

Click **Auto Fixi** 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.

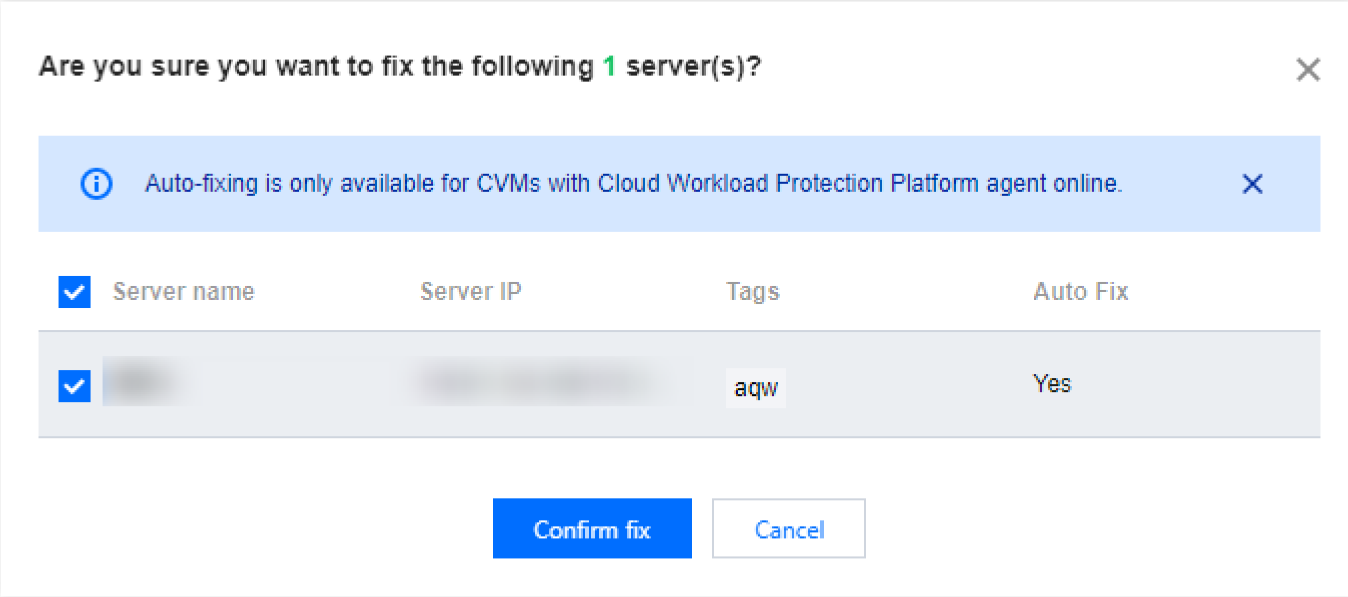
Reference Https://www.phpmyadmin.net/security/PMASA-2016-19/

Affected servers

□	Server IP/Name	Ve...	Server tag	Serve...	Description	First dete...	Last scan...	Status
□	[redacted]	CWPP...	aqw	Running	There is a...	2022-08-01 11:28:43	2022-08-30 18:01:52	⊖ To be fixe

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.



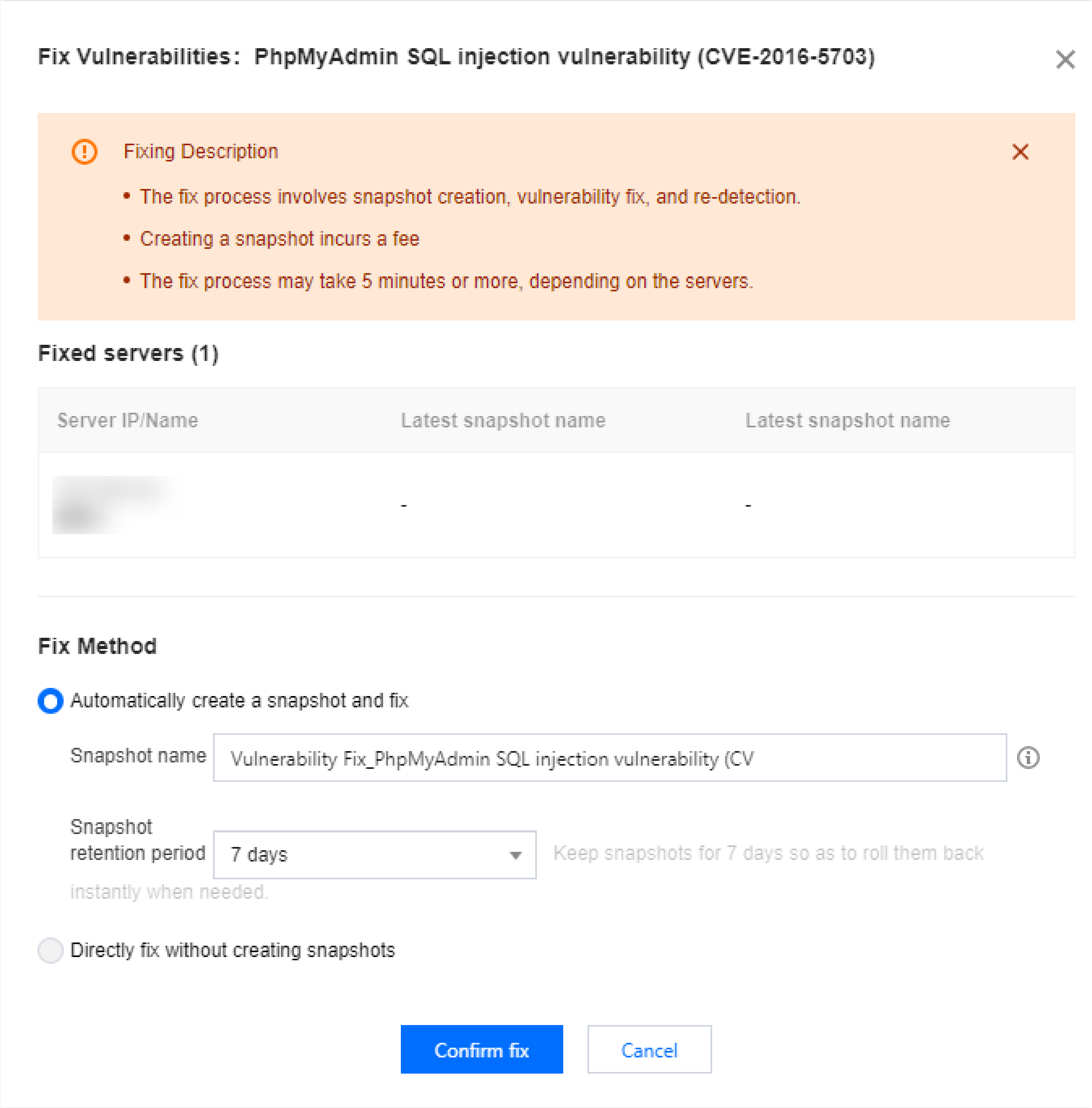
Are you sure you want to fix the following 1 server(s)?

Auto-fixing is only available for CVMs with Cloud Workload Protection Platform agent online.

☑	Server name	Server IP	Tags	Auto Fix
☑	[redacted]	[redacted]	aqw	Yes

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
[redacted]	-	-

Fix Method

● Automatically create a snapshot and fix

Snapshot name: Vulnerability Fix_PhpMyAdmin SQL injection vulnerability (CV

Snapshot retention period: 7 days

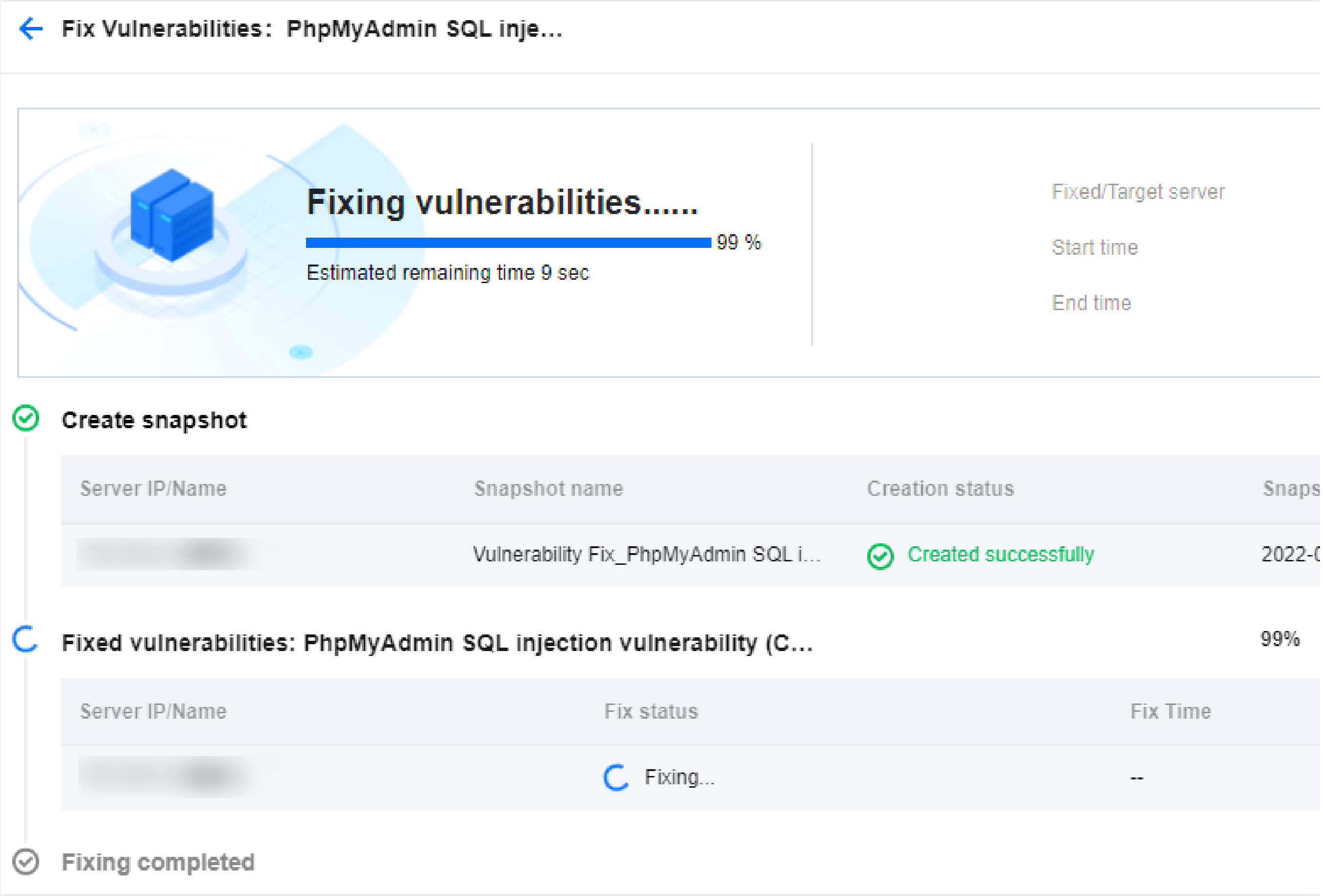
Keep snapshots for 7 days so as to roll them back instantly when needed.

○ 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

Start time

End time

✓ Create snapshot

Server IP/Name	Snapshot name	Creation status	Snaps
	Vulnerability Fix_PhpMyAdmin SQL i...	✓ Created successfully	2022-(

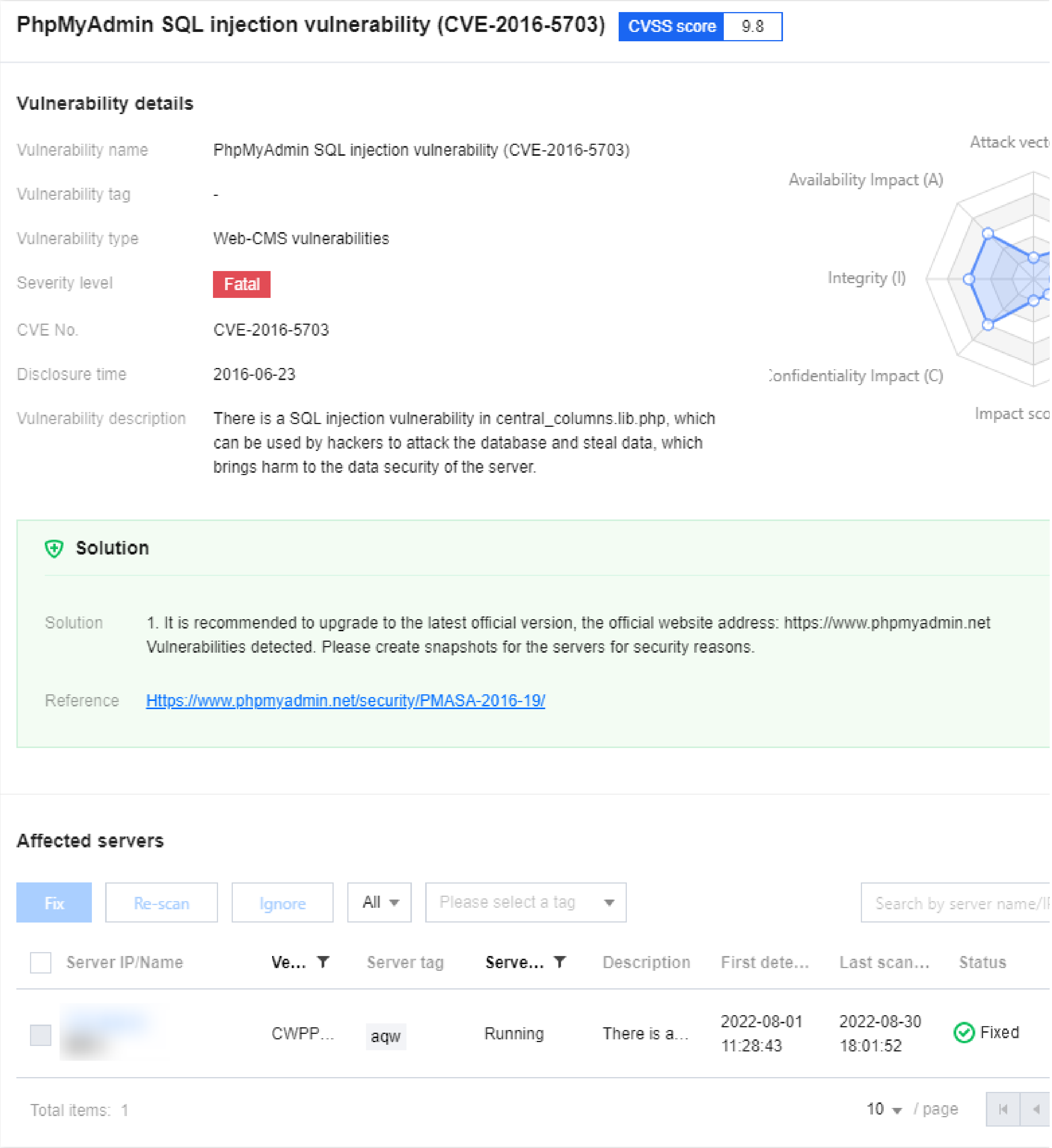
Fixed vulnerabilities: PhpMyAdmin SQL injection vulnerability (C... 99%

Server IP/Name	Fix status	Fix Time
	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/PMASA-2016-19/

Affected servers

□ Server IP/Name	Ve...	Server tag	Serve...	Description	First dete...	Last scan...	Status
□ [redacted]	CWPP...	aqw	Running	There is a...	2022-08-01 11:28:43	2022-08-30 18:01:52	✓ Fixed

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.