Cisco Crosswork Patch for Apache Log4j Vulnerability

First Published: 2021-12-21

This document provides information about the patch releases to resolve the Apache Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45046) in Cisco Crosswork products.

Overview

Problem Summary

The Log4j vulnerability impacts Java-based microservices and UI plugins in Crosswork Platform Infrastructure and Crosswork Applications.

- CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker-controlled LDAP and other JNDI related endpoints.
- CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack.

Resolution

Every microservice using the vulnerable version is upgraded to Log4j version 2.16.0.

Patch Release Versions for Cisco Crosswork Products

The patch files (.tar.gz) are available on the Cisco Software Download page.

Table 1: Patch Releases

Cisco Crosswork Product	Impacted Production Releases	Defect ID	Release Versions
Crosswork Infrastructure	4.0.0 4.1.0	CSCwa47367	4.0.1 4.1.1

Cisco Crosswork Product	Impacted Production Releases	Defect ID	Release Versions
Crosswork Data Gateway (on-premise)	2.0.0 3.0.0	CSCwa47257	**Note** Log4j patch for Crosswork Data Gateway versions 2.0.0 and 3.0.0 is part of Crosswork Infrastructure Log4j patch versions 4.0.1 and 4.1.1 respectively. The Crosswork Infrastructure patch delivers related fixes for Crosswork Data Gateway automatically after activation.
Crosswork Data Gateway (Cloud applications)	2.0.1	CSCwa47257	2.0.2 **Note** The latest release of Crosswork Data Gateway for Cloud applications is 3.0.1.
Crosswork Network Controller	2.0.0 3.0.0	CSCwa49936	2.0.1 3.0.1
Crosswork Optimization Engine	2.0.0 3.0.0	CSCwa49939	2.1.0 3.1.0
Crosswork Zero Touch Provisioning	2.0.0 3.0.0	CSCwa47259	2.0.1 3.0.1

Patch Installation Workflow

This section explains how to install patch files from the Cisco Crosswork UI.

Before you begin, ensure that you have the following:

- Patch image file (.tar.gz) downloaded from Cisco Software Download to your local machine.
- Cisco Crosswork Administrator user credentials.
- Management IP address used for your Crosswork VM deployment.

Note If you encounter any error while installing the patch, please contact the Cisco Customer Experience team.

Procedure

Step 1 Click on **Administration** > **Crosswork Management**, and select the **Application Management** tab. The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

Step 2 Click on the **Add File (.tar.gz)** option to add the patch file that you had downloaded.

Step 3 In the Add File dialog box, enter the relevant information and click **Add**.

Step 4 Once the file is added, you can observe the existing application tile (in this example, Zero Touch Provisioning) displaying an upgrade prompt.



To upgrade, click the upgrade prompt and the patch file is installed.

Step 5 Alternatively, click ··· on the application tile, and select the **Upgrade** option from the drop down list.



In the Upgrade popup screen, select the new version that you want to upgrade to, and click **Upgrade**. Click on **Job History** to see the progress of the upgrade operation.

Step 6 **Additional installation steps for Crosswork Infrastructure 4.0.1 patch:**

Note
The following steps are applicable only for Crosswork Infrastructure 4.0.1 patch image (`cw-na-infra-patch-4.0.1-5-release-211222.tar.gz`) and are not needed for any other patch file.

a) Download Crosswork Infrastructure 4.0.1 patch image (`cw-na-infra-patch-4.0.1-5-release-211222.tar.gz`) from cisco.com into any linux server.

b) Verify the checksum before proceeding. Hover the cursor over the image file and copy the checksum (either MD5 or SHA512) from cisco.com. Execute the below commands to check the file integrity.

```
cd <directory consisting .tar.gz file>
md5sum ./cw-na-infra-script-4.0.1.tar.gz
(OR)
sha512sum ./cw-na-infra-script-4.0.1.tar.gz
```

Compare the checksum displayed against the value copied from cisco.com.

c) Unzip the patch image file.

```
cd <folder where tar was download>
tar -xvf ./cw-na-infra-script-4.0.1.tar.gz
```

The following files (bash script and instructions) are displayed:

```
-- cw-na-infra-script-4.0.1.sh
-- README.txt
```

d) Execute the following commands from the directory containing the bash script.

```
scp ./cw-na-infra-script-4.0.1.sh cw-admin@<cw mgmt-ip>:/home/cw-admin/
```

Note
Replace `<cw mgmt-ip>` with the management IP address used for your Crosswork deployment.

e) Execute the bash script.

Note
The script requires user input, follow instructions as per script execution.

```
cd /home/cw-admin
chmod +x ./cw-na-infra-script-4.0.1.sh
./cw-na-infra-script-4.0.1.sh
```

This script restarts the Crosswork Infrastructure pods that were patched for the new patched image to take effect. Monitor the script and enter **yes** for each of the pods as prompted.

© 2021 Cisco Systems, Inc. All rights reserved.