Cisco Crosswork Patch for Spring4Shell Vulnerability

First Published: 2022-05-04

Last Modified: 2023-01-16

This document provides information about the patch releases to resolve the Spring4Shell vulnerabilities (CVE-2022-22965) in Cisco Crosswork products.

Overview

Problem Summary

The Spring4Shell vulnerability impacts a Spring MVC or Spring WebFlux application running on JDK 9+ that may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar (for example, the default), it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

- CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+ vulnerability.

Resolution

Every Microservice impacted is upgraded to Spring Framework versions 5.3.18 or 5.2.20. For older applications, running on Tomcat with an unsupported Spring Framework version, Apache Tomcat is upgraded to versions 10.0.20, 9.0.62, or 8.5.78 along with Disallowed Fields setting.

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	New Releases with Fix	Defect ID
Crosswork Infrastructure	4.0.2 4.1.3 **4.1.4**	CSCwb57249 CSCwb70153 CSCwa92197
Crosswork Network Controller	2.0.2 3.0.2 3.0.3	CSCwb43703 CSCwb77371

Cisco Crosswork Product	New Releases with Fix	Defect ID
Crosswork Optimization Engine	2.1.1 3.1.1	CSCwb43709
Cisco Crosswork Change Automation and Health Insights	Only Crosswork Infrastructure patches are required	n/a
Cisco Network Services Orchestrator	5.4.6 5.5.5	n/a
Crosswork Zero Touch Provisioning	2.0.2 3.0.2	CSCwb43706
Crosswork Data Gateway	There is no attack vector for Crosswork Data Gateway. Use the released versions.	n/a

Note Once a VPN Profile is deleted, it cannot be recreated from Service Provision UI form in Crosswork Network Controller. Attempting to recreate it from UI fails with the message "No Configuration Change Detected". The bug is specific to VPN profiles (/l3vpn-ntw:l3vpn-ntw/vpn-profiles/valid-provider-identifiers/routing-profile-identifier) in Crosswork Network Controller 3.0.2 UI only.

To address this issue, use one of the workarounds below:

- **Workaround 1**: If a VPN Profile is deleted, delete the corresponding Route Policy as well and recreate the Route Policy. This will automatically create the VPN Profile.
- **Workaround 2**: Use the RESTCONF API to create the VPN Profile. This is a Cisco Crosswork Network Controller UI only issue.
- **Workaround 3**: In the Cisco Crosswork Network Controller UI, import the payload directly to create the VPN Profile.

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.

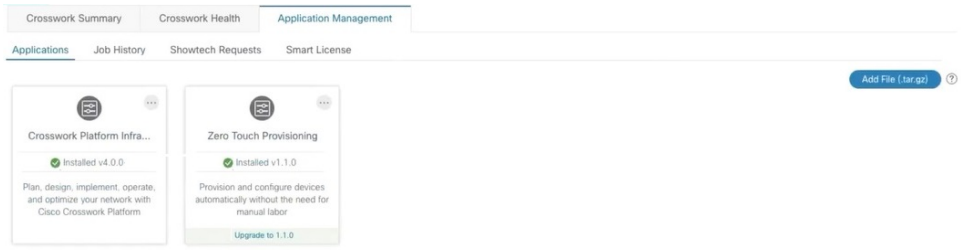
Procedure

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.

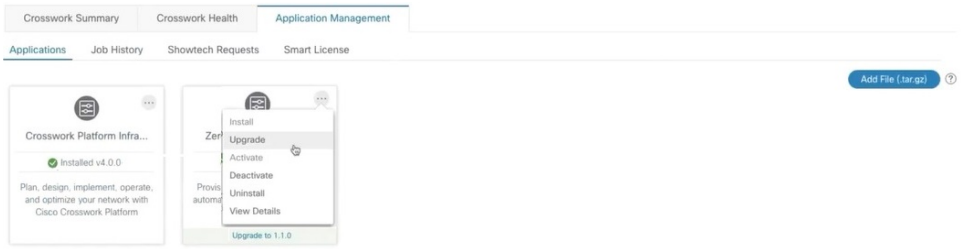
Step 3 In the Add File dialog box, enter the relevant information and click **Add**.

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 pop up 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 4.0.2 patch:**

Note The following steps are applicable only for Crosswork Infrastructure 4.0.2 patch image (`cw-na-infra-patch-4.0.2-4-release-220503.tar.gz`) and are not needed for any other patch file.

a) Download Crosswork Infrastructure 4.0.2 patch image (`cw-na-infra-patch-4.0.2-4-release-220503.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-patch-4.0.2-4-release-220503.tar.gz
(OR)
sha512sum ./cw-na-infra-patch-4.0.2-4-release-220503.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-4.0.2.tar.gz
```

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

```
-- cw-na-infra-script-4.0.2.sh
-- README.txt
```

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

```
scp ./cw-na-infra-script-4.0.2.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-4.0.2.sh
./cw-na-infra-script-4.0.2.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.