Cisco Security Advisory

Cisco Nexus Dashboard Fabric Controller Arbitrary Command Execution Vulnerability

Critical

Advisory ID:
cisco-sa-ndfc-cmdinj-UvYZrKfr

First Published:
2024 October 2 16:00 GMT

Last Updated:
2026 March 31 18:47 GMT

Version 1.1: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwj10299

CVE-2024-20432

CWE-77

CVSS Score:
Base 9.9

Download CSAF

Email

Summary

A vulnerability in the REST API and web UI of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to perform a command injection attack against an affected device.

This vulnerability is due to improper user authorization and insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted commands to an affected REST API endpoint or through the web UI. A successful exploit could allow the attacker to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with *network-admin* privileges.

Note: This vulnerability does not affect Cisco NDFC when it is configured for storage area network (SAN) controller deployment.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr

Affected Products

Vulnerable Products

This vulnerability affects Cisco NDFC.

Note: This vulnerability does not affect Cisco NDFC when it is configured for SAN controller deployment.

Note: Cisco NDFC releases 11.5 and earlier were known as Cisco Data Center Network Manager (DCNM).

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- Nexus Dashboard Insights
- Nexus Dashboard Orchestrator (NDO)

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Releases

In the following table, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco NDFC Release	First Fixed Release
11.5 and earlier	Migrate to a fixed release.
12.0	12.2.2

Note: Starting with Cisco Nexus Dashboard Release 3.1(1k), Cisco NDFC is distributed in Cisco Nexus Dashboard unified releases. Cisco Nexus Dashboard Release 3.2(1e) includes Cisco NDFC Release 12.2.2.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was found during internal security testing by Nate Dunlap of the Cisco Advanced Security Initiatives Group (ASIG).

Cisco would also like to thank Deepanshu Chouhan and Jenis Modi of the Security Assurance Department, Rakuten Mobile Inc. for independently reporting this vulnerability.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr

Revision History

Version	Description	Section	Status	Date
1.1	Updated information about Release 11.5 (DCNM). Updated source information.	Vulnerable Products, Fixed Releases, and Source	Final	2026-MAR-31
1.0	Initial public release.	-	Final	2024-OCT-02

Legal Disclaimer

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

Related to This Advisory