Cisco Security Advisory

Cisco IoT Field Network Director Vulnerabilities

Advisory ID:
cisco-sa-iot-fnd-dos-n8N26Q4u

First Published:
2026 May 6 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwm80968 , CSCwm81008 , CSCwm81015

CVE-2026-20167

CVE-2026-20168

CVE-2026-20169

CWE-284

CWE-388

CWE-77

CVSS Score:
Base 7.7

Download CSAF Email

Summary

Multiple vulnerabilities in the web-based management interface of Cisco IoT Field Network Director Software could allow an authenticated, remote attacker to access files, execute commands, and cause denial of service (DoS) conditions on managed routers.

For more information about these vulnerabilities, see the Details section of this advisory.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iot-fnd-dos-n8N26Q4u

Affected Products

Vulnerable Products

These vulnerabilities affect Cisco IoT Field Network Director, regardless of device configuration.

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 these vulnerabilities.

Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerabilities.

Details about the vulnerabilities are as follows:

CVE-2026-20167: Cisco IoT Field Network Director Remote Device DoS Vulnerability

A vulnerability in the web-based management interface of Cisco IoT Field Network Director could allow an authenticated, remote attacker with low privileges to cause a DoS condition on a remotely managed router.

This vulnerability is due to improper error handling. An attacker could exploit this vulnerability by submitting crafted input to the web-based management interface. A successful exploit could allow the attacker to request unauthorized files from a remote router, causing the router to reload and resulting in a DoS condition.

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

Bug ID(s): CSCwm81015
CVE ID: CVE-2026-20167
Security Impact Rating (SIR): High
CVSS Base Score: 7.7
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2026-20168: Cisco IoT Field Network Director Path Traversal Vulnerability

A vulnerability in the web-based management interface of Cisco IoT Field Network Director could allow an authenticated, remote attacker with low privileges to retrieve files that they do not have permission to access.

This vulnerability is due to insufficient file access checks. An attacker could exploit this vulnerability by submitting crafted input in the web-based management interface. A successful exploit could allow the attacker to read files that they are not authorized to access.

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

Bug ID(s): CSCwm81008
CVE ID: CVE-2026-20168
Security Impact Rating (SIR): Medium
CVSS Base Score: 6.5
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2026-20169: Cisco IoT Field Network Director Command Injection Vulnerability

A vulnerability in the web-based management interface of Cisco IoT Field Network Director could allow an authenticated, remote attacker with low privileges to access files and execute commands on a remote router.

This vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by submitting crafted input in the web-based management interface. A successful exploit could allow the attacker to create, read, or delete files and execute limited commands in user EXEC mode on a remote router.

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

Bug ID(s): CSCwm80968
CVE ID: CVE-2026-20169
Security Impact Rating (SIR): Medium
CVSS Base Score: 6.4
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

Workarounds

There are no workarounds that address these vulnerabilities.

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 these vulnerabilities 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 vulnerabilities that are described in this advisory and the first release that includes the fix for these vulnerabilities. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco IoT Field Network Director Release	First Fixed Release
4 and earlier[1]	Migrate to a fixed release.
5	5.0.0-117

1. Cisco IoT FND Software releases 4.12 and earlier have reached end of software maintenance. Customers are advised to migrate to a supported release that includes the fix for these vulnerabilities.

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 vulnerabilities that are described in this advisory.

Source

Cisco would like to thank Ben Sina for reporting these vulnerabilities.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iot-fnd-dos-n8N26Q4u

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-MAY-06

Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance Center (TAC). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN " AS IS" BASIS. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Quick Links

About Cisco