



# CVE-2018-0308

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2018-0308   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | psirt@cisco.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2018-06-20 21:29:00 UTC   |
| <b>Updated</b>         | 2019-10-09 23:31:00 UTC   |
| <b>Description</b>     | A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an |

## Risk And Classification

**Problem Types: CWE-119**

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product                 | Version          | Update | Edition | Language |
|------------------|--------|-------------------------|------------------|--------|---------|----------|
| Hardware         | Cisco  | Firepower 9000          | -                | All    | All     | All      |
| Hardware         | Cisco  | Firepower 9000          | -                | All    | All     | All      |
| Operating System | Cisco  | Firepower 9000 Firmware | r211             | All    | All     | All      |
| Operating System | Cisco  | Firepower 9000 Firmware | r231             | All    | All     | All      |
| Operating System | Cisco  | Firepower 9000 Firmware | r211             | All    | All     | All      |
| Operating System | Cisco  | Firepower 9000 Firmware | r231             | All    | All     | All      |
| Hardware         | Cisco  | Nexus 5000              | -                | All    | All     | All      |
| Hardware         | Cisco  | Nexus 5000              | -                | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 7.0(0)hsk(0.357) | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 7.0(0)hsk(0.357) | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 7.3(0)d1(0.98)   | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 7.3(0)d1(0.98)   | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 8.1(0.2)s0       | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 8.1(0.2)s0       | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 7.0(0)hsk(0.357) | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 7.3(0)d1(0.98)   | All    | All     | All      |
| Operating System | Cisco  | Nexus 5000 Firmware     | 8.1(0.2)s0       | All    | All     | All      |

|                  |       |                                   |                  |     |     |     |
|------------------|-------|-----------------------------------|------------------|-----|-----|-----|
| Hardware         | Cisco | Nexus 7000                        | -                | All | All | All |
| Hardware         | Cisco | Nexus 7000                        | -                | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 7.3(2)d1(0.49)   | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 7.3(2)d1(0.49)   | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 8.0(1)           | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 8.0(1)           | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 8.1(0.112)s0     | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 8.1(0.112)s0     | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 7.3(2)d1(0.49)   | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 8.0(1)           | All | All | All |
| Operating System | Cisco | Nexus 7000 Firmware               | 8.1(0.112)s0     | All | All | All |
| Hardware         | Cisco | Nexus 9000                        | -                | All | All | All |
| Hardware         | Cisco | Nexus 9000                        | -                | All | All | All |
| Operating System | Cisco | Nexus 9000 Firmware               | 8.1(0)bd(0.20)   | All | All | All |
| Operating System | Cisco | Nexus 9000 Firmware               | 8.1(1)s4         | All | All | All |
| Operating System | Cisco | Nexus 9000 Firmware               | 8.1(0)bd(0.20)   | All | All | All |
| Operating System | Cisco | Nexus 9000 Firmware               | 8.1(1)s4         | All | All | All |
| Operating System | Cisco | Nexus 9000 Firmware               | 8.1(0)bd(0.20)   | All | All | All |
| Operating System | Cisco | Nexus 9000 Firmware               | 8.1(1)s4         | All | All | All |
| Hardware         | Cisco | Unified Computing System          | -                | All | All | All |
| Hardware         | Cisco | Unified Computing System          | -                | All | All | All |
| Operating System | Cisco | Unified Computing System Firmware | 3.1(3a)a         | All | All | All |
| Operating System | Cisco | Unified Computing System Firmware | 3.1(3a)a         | All | All | All |
| Operating System | Cisco | Unified Computing System Firmware | 7.0(0)hsk(0.357) | All | All | All |
| Operating System | Cisco | Unified Computing System Firmware | 7.0(0)hsk(0.357) | All | All | All |
| Operating System | Cisco | Unified Computing System Firmware | 3.1(3a)a         | All | All | All |
| Operating System | Cisco | Unified Computing System Firmware | 7.0(0)hsk(0.357) | All | All | All |

## References

### Reference

Malformed Request

Cisco NX-OS Multiple Bugs Let Remote Users Deny Service and Execute Arbitrary Code and Let Remote Authenticated Users Gain Elevated

Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**