



# CVE-2019-1808

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2019-1808   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | psirt@cisco.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2019-05-15 23:29:00 UTC   |
| <b>Updated</b>         | 2023-03-24 17:46:00 UTC   |
| <b>Description</b>     | A vulnerability in the Image Signature Verification feature of Cisco NX-OS Software could allow an authenticated, local attac |

## Risk And Classification

**Problem Types: CWE-347**

## NVD Known Affected Configurations (CPE 2.3)

| Type     | Vendor | Product      | Version | Update | Edition | Language |
|----------|--------|--------------|---------|--------|---------|----------|
| Hardware | Cisco  | 7000 10-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 10-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 18-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 18-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 4-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 4-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 9-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7000 9-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 10-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 10-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 18-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 18-slot | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 2-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 2-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 6-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | 7700 6-slot  | -       | All    | All     | All      |
| Hardware | Cisco  | Mds 9706     | -       | All    | All     | All      |

|          |       |                |   |     |     |     |
|----------|-------|----------------|---|-----|-----|-----|
| Hardware | Cisco | Mds 9706       | - | All | All | All |
| Hardware | Cisco | Mds 9710       | - | All | All | All |
| Hardware | Cisco | Mds 9710       | - | All | All | All |
| Hardware | Cisco | Mds 9718       | - | All | All | All |
| Hardware | Cisco | Mds 9718       | - | All | All | All |
| Hardware | Cisco | N77-f312ck-26  | - | All | All | All |
| Hardware | Cisco | N77-f312ck-26  | - | All | All | All |
| Hardware | Cisco | N77-f324fq-25  | - | All | All | All |
| Hardware | Cisco | N77-f324fq-25  | - | All | All | All |
| Hardware | Cisco | N77-f348xp-23  | - | All | All | All |
| Hardware | Cisco | N77-f348xp-23  | - | All | All | All |
| Hardware | Cisco | N77-f430cq-36  | - | All | All | All |
| Hardware | Cisco | N77-f430cq-36  | - | All | All | All |
| Hardware | Cisco | N77-m312cq-26l | - | All | All | All |
| Hardware | Cisco | N77-m312cq-26l | - | All | All | All |
| Hardware | Cisco | N77-m324fq-25l | - | All | All | All |
| Hardware | Cisco | N77-m324fq-25l | - | All | All | All |
| Hardware | Cisco | N77-m348xp-23l | - | All | All | All |
| Hardware | Cisco | N77-m348xp-23l | - | All | All | All |
| Hardware | Cisco | N7k-f248xp-25e | - | All | All | All |
| Hardware | Cisco | N7k-f248xp-25e | - | All | All | All |
| Hardware | Cisco | N7k-f306ck-25  | - | All | All | All |
| Hardware | Cisco | N7k-f306ck-25  | - | All | All | All |
| Hardware | Cisco | N7k-f312fq-25  | - | All | All | All |
| Hardware | Cisco | N7k-f312fq-25  | - | All | All | All |
| Hardware | Cisco | N7k-m202cf-22l | - | All | All | All |
| Hardware | Cisco | N7k-m202cf-22l | - | All | All | All |
| Hardware | Cisco | N7k-m206fq-23l | - | All | All | All |
| Hardware | Cisco | N7k-m206fq-23l | - | All | All | All |
| Hardware | Cisco | N7k-m224xp-23l | - | All | All | All |
| Hardware | Cisco | N7k-m224xp-23l | - | All | All | All |
| Hardware | Cisco | N7k-m324fq-25l | - | All | All | All |
| Hardware | Cisco | N7k-m324fq-25l | - | All | All | All |
| Hardware | Cisco | N7k-m348xp-25l | - | All | All | All |
| Hardware | Cisco | N7k-m348xp-25l | - | All | All | All |

|                  |       |                          |     |     |     |     |
|------------------|-------|--------------------------|-----|-----|-----|-----|
| Hardware         | Cisco | Nexus 7000 Supervisor 1  | -   | All | All | All |
| Hardware         | Cisco | Nexus 7000 Supervisor 1  | -   | All | All | All |
| Hardware         | Cisco | Nexus 7000 Supervisor 2  | -   | All | All | All |
| Hardware         | Cisco | Nexus 7000 Supervisor 2  | -   | All | All | All |
| Hardware         | Cisco | Nexus 7000 Supervisor 2e | -   | All | All | All |
| Hardware         | Cisco | Nexus 7000 Supervisor 2e | -   | All | All | All |
| Hardware         | Cisco | Nexus 7700 Supervisor 2e | -   | All | All | All |
| Hardware         | Cisco | Nexus 7700 Supervisor 2e | -   | All | All | All |
| Hardware         | Cisco | Nexus 7700 Supervisor 3e | -   | All | All | All |
| Hardware         | Cisco | Nexus 7700 Supervisor 3e | -   | All | All | All |
| Operating System | Cisco | Nx-os                    | All | All | All | All |
| Operating System | Cisco | Nx-os                    | All | All | All | All |

## References

| Reference  | Source |
|--|--------|
| Malformed Request  | BID    |
| Cisco MDS 9700 Series Multilayer Directors and Nexus 7000/7700 Series Switches Software Patch Signature Verification Vulnerability | CISCO  |
| CVE Program record   | CVE    |
| NVD vulnerability detail   | NVD    |

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](#)