



CVE-2019-1977

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2019-1977 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-08-30 09:15:00 UTC |
| Updated | 2019-10-09 23:48:00 UTC |
| Description | A vulnerability within the Endpoint Learning feature of Cisco Nexus 9000 Series Switches running in Application Centric Infr |

Risk And Classification

Problem Types: CWE-371

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|----------|--------|------------------|---------|--------|---------|----------|
| Hardware | Cisco | Nexus 9000 | - | All | All | All |
| Hardware | Cisco | Nexus 9000 | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-fx | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-fx | - | All | All | All |
| Hardware | Cisco | Nexus 93120tx | - | All | All | All |
| Hardware | Cisco | Nexus 93120tx | - | All | All | All |
| Hardware | Cisco | Nexus 93128tx | - | All | All | All |
| Hardware | Cisco | Nexus 93128tx | - | All | All | All |
| Hardware | Cisco | Nexus 93180lc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93180lc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-fx | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-fx | - | All | All | All |
| Hardware | Cisco | Nexus 9332pq | - | All | All | All |

| | | | | | | |
|------------------|-------|------------------|----------|-----|-----|-----|
| Hardware | Cisco | Nexus 9332pq | - | All | All | All |
| Hardware | Cisco | Nexus 9336c-fx2 | - | All | All | All |
| Hardware | Cisco | Nexus 9336c-fx2 | - | All | All | All |
| Hardware | Cisco | Nexus 9336pq | - | All | All | All |
| Hardware | Cisco | Nexus 9336pq | - | All | All | All |
| Hardware | Cisco | Nexus 9348gc-fxp | - | All | All | All |
| Hardware | Cisco | Nexus 9348gc-fxp | - | All | All | All |
| Hardware | Cisco | Nexus 9364c | - | All | All | All |
| Hardware | Cisco | Nexus 9364c | - | All | All | All |
| Hardware | Cisco | Nexus 9372px | - | All | All | All |
| Hardware | Cisco | Nexus 9372px | - | All | All | All |
| Hardware | Cisco | Nexus 9372px-e | - | All | All | All |
| Hardware | Cisco | Nexus 9372px-e | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx-e | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx-e | - | All | All | All |
| Hardware | Cisco | Nexus 9396px | - | All | All | All |
| Hardware | Cisco | Nexus 9396px | - | All | All | All |
| Hardware | Cisco | Nexus 9396tx | - | All | All | All |
| Hardware | Cisco | Nexus 9396tx | - | All | All | All |
| Hardware | Cisco | Nexus 9504 | - | All | All | All |
| Hardware | Cisco | Nexus 9504 | - | All | All | All |
| Hardware | Cisco | Nexus 9508 | - | All | All | All |
| Hardware | Cisco | Nexus 9508 | - | All | All | All |
| Hardware | Cisco | Nexus 9516 | - | All | All | All |
| Hardware | Cisco | Nexus 9516 | - | All | All | All |
| Operating System | Cisco | Nx-os | 12.3(1h) | All | All | All |
| Operating System | Cisco | Nx-os | 12.3(1h) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1(2m) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1(2o) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1(2p) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1(2m) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1(2o) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1(2p) | All | All | All |

| | | | | | | |
|------------------|-------|-------|------------|-----|-----|-----|
| Operating System | Cisco | Nx-os | 12.3\ (1h) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1\ (2m) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1\ (2o) | All | All | All |
| Operating System | Cisco | Nx-os | 13.1\ (2p) | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|------------|
| Cisco Nexus 9000 Series Fabric Switches ACI Mode Border Leaf Endpoint Learning Vulnerability | CISCO | tools.cisco.com | Vendor Ad |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report