



CVE-2023-20089

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-20089 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-02-23 20:15:00 UTC |
| Updated | 2023-11-07 04:06:00 UTC |
| Description | A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Applicat |

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|----------|--------|---------------------|---------|--------|---------|----------|
| Hardware | Cisco | Nexus 9000v | - | All | All | All |
| Hardware | Cisco | Nexus 92160yc-x | - | All | All | All |
| Hardware | Cisco | Nexus 92300yc | - | All | All | All |
| Hardware | Cisco | Nexus 92304qc | - | All | All | All |
| Hardware | Cisco | Nexus 92348gc-x | - | All | All | All |
| Hardware | Cisco | Nexus 9236c | - | All | All | All |
| Hardware | Cisco | Nexus 9272q | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-ex-24 | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-fx | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-fx-24 | - | All | All | All |
| Hardware | Cisco | Nexus 93108tc-fx3p | - | All | All | All |
| Hardware | Cisco | Nexus 93120tx | - | All | All | All |
| Hardware | Cisco | Nexus 93128tx | - | All | All | All |
| Hardware | Cisco | Nexus 9316d-gx | - | All | All | All |
| Hardware | Cisco | Nexus 93180lc-ex | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-ex | - | All | All | All |

| | | | | | | |
|------------------|-------|------------------------|----------|-----|-----|-----|
| Hardware | Cisco | Nexus 93180yc-ex-24 | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-fx | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-fx-24 | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-fx3 | - | All | All | All |
| Hardware | Cisco | Nexus 93180yc-fx3s | - | All | All | All |
| Hardware | Cisco | Nexus 93216tc-fx2 | - | All | All | All |
| Hardware | Cisco | Nexus 93240yc-fx2 | - | All | All | All |
| Hardware | Cisco | Nexus 9332c | - | All | All | All |
| Hardware | Cisco | Nexus 9332d-gx2b | - | All | All | All |
| Hardware | Cisco | Nexus 9332pq | - | All | All | All |
| Hardware | Cisco | Nexus 93360yc-fx2 | - | All | All | All |
| Hardware | Cisco | Nexus 9336c-fx2 | - | All | All | All |
| Hardware | Cisco | Nexus 9336c-fx2-e | - | All | All | All |
| Hardware | Cisco | Nexus 9336pq Aci Spine | - | All | All | All |
| Hardware | Cisco | Nexus 9348d-gx2a | - | All | All | All |
| Hardware | Cisco | Nexus 9348gc-fxp | - | All | All | All |
| Hardware | Cisco | Nexus 93600cd-gx | - | All | All | All |
| Hardware | Cisco | Nexus 9364c | - | All | All | All |
| Hardware | Cisco | Nexus 9364c-gx | - | All | All | All |
| Hardware | Cisco | Nexus 9364d-gx2a | - | All | All | All |
| Hardware | Cisco | Nexus 9372px | - | All | All | All |
| Hardware | Cisco | Nexus 9372px-e | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx-e | - | All | All | All |
| Hardware | Cisco | Nexus 9396px | - | All | All | All |
| Hardware | Cisco | Nexus 9396tx | - | All | All | All |
| Hardware | Cisco | Nexus 9408 | - | All | All | All |
| Hardware | Cisco | Nexus 9508 | - | All | All | All |
| Hardware | Cisco | Nexus 9808 | - | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\1g\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\2e\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\2f\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\2g\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\2h\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\3e\ | All | All | All |

| | | | | | | |
|------------------|-------|-------|----------|-----|-----|-----|
| Operating System | Cisco | Nx-os | 15.2\3f\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\3g\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\4d\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\4e\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\4f\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\5c\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\5d\ | All | All | All |
| Operating System | Cisco | Nx-os | 15.2\5e\ | All | All | All |
| Operating System | Cisco | Nx-os | 16.0\1g\ | All | All | All |
| Operating System | Cisco | Nx-os | 16.0\1j\ | All | All | All |

References

| Reference | Source |
|---|--------|
| Cisco Nexus 9000 Series Fabric Switches in ACI Mode Link Layer Discovery Protocol Memory Leak Denial of Service Vulnerability | CISCO |
| CVE Program record | CVE.OF |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317296 Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode Link Layer Discovery Protocol (LLDP) Memory Leak Denial of Service (DoS) Vulnerability (cisco-sa-aci-ldp-dos-ySCNZOpX)

© 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