



CVE-2019-1726

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

Summary

CVE	CVE-2019-1726
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-15 17:29:00 UTC
Updated	2020-10-09 17:03:00 UTC
Description	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to access internal services th

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Mds 9000	-	All	All	All
Hardware	Cisco	Mds 9000	-	All	All	All
Hardware	Cisco	Mds 9100	-	All	All	All
Hardware	Cisco	Mds 9100	-	All	All	All
Hardware	Cisco	Mds 9200	-	All	All	All
Hardware	Cisco	Mds 9200	-	All	All	All
Hardware	Cisco	Mds 9500	-	All	All	All
Hardware	Cisco	Mds 9500	-	All	All	All
Hardware	Cisco	Mds 9700	-	All	All	All
Hardware	Cisco	Mds 9700	-	All	All	All
Hardware	Cisco	Nexus 3000	-	All	All	All
Hardware	Cisco	Nexus 3000	-	All	All	All
Hardware	Cisco	Nexus 3100	-	All	All	All
Hardware	Cisco	Nexus 3100	-	All	All	All
Hardware	Cisco	Nexus 3100-z	-	All	All	All
Hardware	Cisco	Nexus 3100-z	-	All	All	All
Hardware	Cisco	Nexus 3100v	-	All	All	All

Hardware	Cisco	Nexus 3100v	-	All	All	All
Hardware	Cisco	Nexus 3200	-	All	All	All
Hardware	Cisco	Nexus 3200	-	All	All	All
Hardware	Cisco	Nexus 3400	-	All	All	All
Hardware	Cisco	Nexus 3400	-	All	All	All
Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3524-x	-	All	All	All
Hardware	Cisco	Nexus 3524-x	-	All	All	All
Hardware	Cisco	Nexus 3524-xl	-	All	All	All
Hardware	Cisco	Nexus 3524-xl	-	All	All	All
Hardware	Cisco	Nexus 3548-x	-	All	All	All
Hardware	Cisco	Nexus 3548-x	-	All	All	All
Hardware	Cisco	Nexus 3548-xl	-	All	All	All
Hardware	Cisco	Nexus 3548-xl	-	All	All	All
Hardware	Cisco	Nexus 3600	-	All	All	All
Hardware	Cisco	Nexus 3600	-	All	All	All
Hardware	Cisco	Nexus 5500	-	All	All	All
Hardware	Cisco	Nexus 5500	-	All	All	All
Hardware	Cisco	Nexus 5600	-	All	All	All
Hardware	Cisco	Nexus 5600	-	All	All	All
Hardware	Cisco	Nexus 6000	-	All	All	All
Hardware	Cisco	Nexus 6000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7700	-	All	All	All
Hardware	Cisco	Nexus 7700	-	All	All	All
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 9200	-	All	All	All
Hardware	Cisco	Nexus 9200	-	All	All	All
Hardware	Cisco	Nexus 9300	-	All	All	All
Hardware	Cisco	Nexus 9300	-	All	All	All
Hardware	Cisco	Nexus 9500	-	All	All	All
Hardware	Cisco	Nexus 9500	-	All	All	All

Operating System	Cisco	Nx-os	All	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All
Hardware	Cisco	Ucs 6248up	-	All	All	All
Hardware	Cisco	Ucs 6248up	-	All	All	All
Hardware	Cisco	Ucs 6296up	-	All	All	All
Hardware	Cisco	Ucs 6296up	-	All	All	All

References

Reference	Source	Link	Tags
Cisco NX-OS Software CVE-2019-1726 Local Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VC
Cisco NX-OS Software CLI Bypass to Internal Service Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[316978](#) Cisco NX-OS Software CLI Bypass to Internal Service Vulnerability(cisco-sa-20190515-nxos-cli-bypass)

© [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](#)