



CVE-2019-1964

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

Summary

CVE	CVE-2019-1964
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-28 19:15:00 UTC
Updated	2019-10-09 23:48:00 UTC
Description	A vulnerability in the IPv6 traffic processing of Cisco NX-OS Software could allow an unauthenticated, remote attacker to ca

Risk And Classification

Problem Types: CWE-20

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	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	Link	Tags
Cisco NX-OS Software IPv6 Denial of 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.

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](#).

Free CVE JSON API cve.report/api

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