CVE-2018-0395

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0395
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-17 19:29:00 UTC
Updated	2023-04-20 17:17:00 UTC
Description	A vulnerability in the Link Layer Discovery Protocol (LLDP) implementation for Cisco FXOS Software and Cisco NX-OS Sof

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Firepower 9300	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Operating System	Cisco	Firepower Extensible Operating System	r231	All	All	All
Operating System	Cisco	Fxos	12.3(1e)	All	All	All
Operating System	Cisco	Fxos	12.3\(1e\)	All	All	All
Operating System	Cisco	Fxos	3.2(3d)c	All	All	All
Operating System	Cisco	Fxos	3.2\(3d\)c	All	All	All
Operating System	Cisco	Fxos	6.0(4)	All	All	All
Operating System	Cisco	Fxos	6.0\(4\)	All	All	All
Operating System	Cisco	Fxos	6.1(3)s2	All	All	All
Operating System	Cisco	Fxos	6.1\(3\)s2	All	All	All
Operating System	Cisco	Fxos	r231	All	All	All
Operating System	Cisco	Fxos	12.3\(1e\)	All	All	All
Operating System	Cisco	Fxos	3.2\(3d\)c	All	All	All
Operating System	Cisco	Fxos	6.0\(4\)	All	All	All
Operating System	Cisco	Fxos	6.1\(3\)s2	All	All	All
Operating System	Cisco	Fxos	r231	All	All	All

Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 4-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 4-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 2-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 2-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 6-slot	-	All	All	All
Hardware	Cisco	Nexus 7700 6-slot	-	All	All	All
Operating System	Cisco	Nx-os	12.3(1e)	All	All	All
Operating System	Cisco	Nx-os	12.3\(1e\)	All	All	All
Operating System	Cisco	Nx-os	3.2(3d)c	All	All	All
Operating System	Cisco	Nx-os	3.2\(3d\)c	All	All	All
Operating System	Cisco	Nx-os	6.0(4)	All	All	All
Operating System	Cisco	Nx-os	6.0\(4\)	All	All	All
Operating System	Cisco	Nx-os	6.1(3)s2	All	All	All
Operating System	Cisco	Nx-os	6.1\(3\)s2	All	All	All
Operating System	Cisco	Nx-os	r231	All	All	All
Operating System	Cisco	Nx-os	12.3\(1e\)	All	All	All
Operating System	Cisco	Nx-os	3.2\(3d\)c	All	All	All
Operating System	Cisco	Nx-os	6.0\(4\)	All	All	All
Operating System	Cisco	Nx-os	6.1\(3\)s2	All	All	All
Operating System	Cisco	Nx-os	r231	All	All	All
Hardware	Cisco	Ucs	-	All	All	All
Hardware	Cisco	Ucs	-	All	All	All

References

Reference	Source	Link

Malformed Request	BID	www.secu
Cisco FXOS and NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability	CISCO	tools.cisc
Cisco NX-OS LLDP TLV Processing Bugs Let Remote Users Cause the Target Service to Crash - SecurityTracker	SECTRACK	www.secu
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

316953 Cisco FXOS and NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability(cisco-sa-20181017-fxnx-os-dos)

730062 Cisco FXOS and NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability(cisco-sa-20181017-fxnx-os-dos)

© 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 registred 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