



CVE-2015-0661

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

Summary

CVE	CVE-2015-0661
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-06 03:00:00 UTC
Updated	2015-11-02 18:28:00 UTC
Description	The SNMPv2 implementation in Cisco IOS XR allows remote authenticated users to cause a denial of service (snmpd daen

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xr	All	All	All	All
Operating System	Cisco	Ios Xr	All	All	All	All

References

Reference	Source	Link
Cisco IOS XR SNMP Processing Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	SECTrack	www.securitytracker.com
Cisco IOS XR Software Malformed SNMP Packet Denial of Service Vulnerability	CISCO	tools.cisco.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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