



CVE-2014-3378

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

Summary

CVE	CVE-2014-3378
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-20 10:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	tacacsd in Cisco IOS XR 5.1 and earlier allows remote attackers to cause a denial of service (process reload) via a malformed

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	2.0	All	All	All
Operating System	Cisco	ios Xr	3.0	All	All	All
Operating System	Cisco	ios Xr	3.0.1	All	All	All
Operating System	Cisco	ios Xr	3.1	All	All	All
Operating System	Cisco	ios Xr	3.1.0	All	All	All
Operating System	Cisco	ios Xr	3.2	All	All	All
Operating System	Cisco	ios Xr	3.2.1	All	All	All
Operating System	Cisco	ios Xr	3.2.2	All	All	All
Operating System	Cisco	ios Xr	3.2.4	All	All	All
Operating System	Cisco	ios Xr	3.2.50	All	All	All
Operating System	Cisco	ios Xr	3.3	All	All	All
Operating System	Cisco	ios Xr	3.3.1	All	All	All
Operating System	Cisco	ios Xr	3.3.2	All	All	All
Operating System	Cisco	ios Xr	3.3.3	All	All	All
Operating System	Cisco	ios Xr	3.3.4	All	All	All
Operating System	Cisco	ios Xr	3.3.5	All	All	All
Operating System	Cisco	ios Xr	3.4	All	All	All

Operating System	Cisco	ios Xr	3.4.1	All	All	All
Operating System	Cisco	ios Xr	3.4.2	All	All	All
Operating System	Cisco	ios Xr	3.4.3	All	All	All
Operating System	Cisco	ios Xr	3.5	All	All	All
Operating System	Cisco	ios Xr	3.5.1	All	All	All
Operating System	Cisco	ios Xr	3.5.2	All	All	All
Operating System	Cisco	ios Xr	3.5.3	All	All	All
Operating System	Cisco	ios Xr	3.5.4	All	All	All
Operating System	Cisco	ios Xr	3.6	All	All	All
Operating System	Cisco	ios Xr	3.6.1	All	All	All
Operating System	Cisco	ios Xr	3.6.2	All	All	All
Operating System	Cisco	ios Xr	3.6.3	All	All	All
Operating System	Cisco	ios Xr	3.7	All	All	All
Operating System	Cisco	ios Xr	3.7.1	All	All	All
Operating System	Cisco	ios Xr	3.7.2	All	All	All
Operating System	Cisco	ios Xr	3.7.3	All	All	All
Operating System	Cisco	ios Xr	3.8.0	All	All	All
Operating System	Cisco	ios Xr	3.8.1	All	All	All
Operating System	Cisco	ios Xr	3.8.2	All	All	All
Operating System	Cisco	ios Xr	3.8.3	All	All	All
Operating System	Cisco	ios Xr	3.8.4	All	All	All
Operating System	Cisco	ios Xr	3.9.0	All	All	All
Operating System	Cisco	ios Xr	3.9.1	All	All	All
Operating System	Cisco	ios Xr	3.9.2	All	All	All
Operating System	Cisco	ios Xr	4.0.0	All	All	All
Operating System	Cisco	ios Xr	4.0.1	All	All	All
Operating System	Cisco	ios Xr	4.0.2	All	All	All
Operating System	Cisco	ios Xr	4.0.3	All	All	All
Operating System	Cisco	ios Xr	4.0.4	All	All	All
Operating System	Cisco	ios Xr	4.1	All	All	All
Operating System	Cisco	ios Xr	4.1.1	All	All	All
Operating System	Cisco	ios Xr	4.1.2	All	All	All
Operating System	Cisco	ios Xr	4.2.0	All	All	All
Operating System	Cisco	ios Xr	4.3.0	All	All	All
Operating System	Cisco	ios Xr	4.3.1	All	All	All

Operating System	Cisco	ios Xr	4.3.2	All	All	All
Operating System	Cisco	ios Xr	4.3.4	All	All	All
Operating System	Cisco	ios Xr	5.1.0	All	All	All
Operating System	Cisco	ios Xr	2.0	All	All	All
Operating System	Cisco	ios Xr	3.0	All	All	All
Operating System	Cisco	ios Xr	3.0.1	All	All	All
Operating System	Cisco	ios Xr	3.1	All	All	All
Operating System	Cisco	ios Xr	3.1.0	All	All	All
Operating System	Cisco	ios Xr	3.2	All	All	All
Operating System	Cisco	ios Xr	3.2.1	All	All	All
Operating System	Cisco	ios Xr	3.2.2	All	All	All
Operating System	Cisco	ios Xr	3.2.4	All	All	All
Operating System	Cisco	ios Xr	3.2.50	All	All	All
Operating System	Cisco	ios Xr	3.3	All	All	All
Operating System	Cisco	ios Xr	3.3.1	All	All	All
Operating System	Cisco	ios Xr	3.3.2	All	All	All
Operating System	Cisco	ios Xr	3.3.3	All	All	All
Operating System	Cisco	ios Xr	3.3.4	All	All	All
Operating System	Cisco	ios Xr	3.3.5	All	All	All
Operating System	Cisco	ios Xr	3.4	All	All	All
Operating System	Cisco	ios Xr	3.4.1	All	All	All
Operating System	Cisco	ios Xr	3.4.2	All	All	All
Operating System	Cisco	ios Xr	3.4.3	All	All	All
Operating System	Cisco	ios Xr	3.5	All	All	All
Operating System	Cisco	ios Xr	3.5.1	All	All	All
Operating System	Cisco	ios Xr	3.5.2	All	All	All
Operating System	Cisco	ios Xr	3.5.3	All	All	All
Operating System	Cisco	ios Xr	3.5.4	All	All	All
Operating System	Cisco	ios Xr	3.6	All	All	All
Operating System	Cisco	ios Xr	3.6.1	All	All	All
Operating System	Cisco	ios Xr	3.6.2	All	All	All
Operating System	Cisco	ios Xr	3.6.3	All	All	All
Operating System	Cisco	ios Xr	3.7	All	All	All
Operating System	Cisco	ios Xr	3.7.1	All	All	All
Operating System	Cisco	ios Xr	3.7.2	All	All	All
Operating System	Cisco	ios Xr	3.7.3	All	All	All

Operating System	Cisco	ios Xr	3.7.3	All	All	All
Operating System	Cisco	ios Xr	3.8.0	All	All	All
Operating System	Cisco	ios Xr	3.8.1	All	All	All
Operating System	Cisco	ios Xr	3.8.2	All	All	All
Operating System	Cisco	ios Xr	3.8.3	All	All	All
Operating System	Cisco	ios Xr	3.8.4	All	All	All
Operating System	Cisco	ios Xr	3.9.0	All	All	All
Operating System	Cisco	ios Xr	3.9.1	All	All	All
Operating System	Cisco	ios Xr	3.9.2	All	All	All
Operating System	Cisco	ios Xr	4.0.0	All	All	All
Operating System	Cisco	ios Xr	4.0.1	All	All	All
Operating System	Cisco	ios Xr	4.0.2	All	All	All
Operating System	Cisco	ios Xr	4.0.3	All	All	All
Operating System	Cisco	ios Xr	4.0.4	All	All	All
Operating System	Cisco	ios Xr	4.1	All	All	All
Operating System	Cisco	ios Xr	4.1.1	All	All	All
Operating System	Cisco	ios Xr	4.1.2	All	All	All
Operating System	Cisco	ios Xr	4.2.0	All	All	All
Operating System	Cisco	ios Xr	4.3.0	All	All	All
Operating System	Cisco	ios Xr	4.3.1	All	All	All
Operating System	Cisco	ios Xr	4.3.2	All	All	All
Operating System	Cisco	ios Xr	4.3.4	All	All	All
Operating System	Cisco	ios Xr	5.1.0	All	All	All

References				
Reference			Source	Link
Security Advisory SA59649 - Cisco IOS XR TACACS+ Packet Handling Denial of Service Vulnerability - Secunia			SECUNIA	secunia.com
Security Advisory SA59632 - Cisco IOS XR TACACS+ Packet Handling Denial of Service Vulnerability - Secunia			SECUNIA	secunia.com
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com
tools.cisco.com/security/center/viewAlert.x			CONFIRM	tools.cisco.com
Cisco IOS XR Packet Processing Flaws Let Remote and Remote Authenticated Users Deny Service - SecurityTracker			SECTRACK	www.securitytracker.com
Cisco IOS XR Software CVE-2014-3378 TACACS+ Packet Parsing Denial of Service Vulnerability			BID	www.bids.cisco.com
20140918 Cisco IOS XR Software Malformed TACACS+ 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.

© [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](#)