



CVE-2017-6718

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

Summary

CVE	CVE-2017-6718
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-04 00:29:00 UTC
Updated	2017-07-07 17:39:00 UTC
Description	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to elevate privileges to the r

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	6.0.2	All	All	All
Operating System	Cisco	Ios Xr	6.0.2.01	All	All	All
Operating System	Cisco	Ios Xr	6.0.2	All	All	All
Operating System	Cisco	Ios Xr	6.0.2.01	All	All	All

References

Reference	Source	Link
Cisco IOS XR Software CVE-2017-6718 Local Privilege Escalation Vulnerability	BID	www.s
Cisco IOS XR Software Privilege Escalation Vulnerability	CONFIRM	tools.ci
Cisco IOS XR Command Injection and File Overwrite Flaws Let Local Users Obtain Root Privileges - SecurityTracker	SECTrack	www.s
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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](#)