



CVE-2020-3473

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

Summary

CVE	CVE-2020-3473
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-04 03:15:00 UTC
Updated	2020-09-09 19:50:00 UTC
Description	A vulnerability in task group assignment for a specific CLI command in Cisco IOS XR Software could allow an authenticated

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	8201	-	All	All	All
Hardware	Cisco	8201	-	All	All	All
Hardware	Cisco	8202	-	All	All	All
Hardware	Cisco	8202	-	All	All	All
Hardware	Cisco	8808	-	All	All	All
Hardware	Cisco	8808	-	All	All	All
Hardware	Cisco	8812	-	All	All	All
Hardware	Cisco	8812	-	All	All	All
Hardware	Cisco	8818	-	All	All	All
Hardware	Cisco	8818	-	All	All	All
Operating System	Cisco	ios Xr	All	All	All	All
Operating System	Cisco	ios Xr	All	All	All	All
Hardware	Cisco	ios Xrv 9000	-	All	All	All
Hardware	Cisco	ios Xrv 9000	-	All	All	All
Hardware	Cisco	Ncs 4009	-	All	All	All
Hardware	Cisco	Ncs 4009	-	All	All	All
Hardware	Cisco	Ncs 4016	-	All	All	All

Hardware	Cisco	Ncs 4016	-	All	All	All
Hardware	Cisco	Ncs 540	-	All	All	All
Hardware	Cisco	Ncs 540	-	All	All	All
Hardware	Cisco	Ncs 5501	-	All	All	All
Hardware	Cisco	Ncs 5501	-	All	All	All
Hardware	Cisco	Ncs 5501-se	-	All	All	All
Hardware	Cisco	Ncs 5501-se	-	All	All	All
Hardware	Cisco	Ncs 5502	-	All	All	All
Hardware	Cisco	Ncs 5502	-	All	All	All
Hardware	Cisco	Ncs 5502-se	-	All	All	All
Hardware	Cisco	Ncs 5502-se	-	All	All	All
Hardware	Cisco	Ncs 5508	-	All	All	All
Hardware	Cisco	Ncs 5508	-	All	All	All
Hardware	Cisco	Ncs 5516	-	All	All	All
Hardware	Cisco	Ncs 5516	-	All	All	All
Hardware	Cisco	Ncs 560	-	All	All	All
Hardware	Cisco	Ncs 560	-	All	All	All
Hardware	Cisco	Ncs 6000	-	All	All	All
Hardware	Cisco	Ncs 6000	-	All	All	All
Hardware	Cisco	Ncs 6008	-	All	All	All
Hardware	Cisco	Ncs 6008	-	All	All	All

References

Reference	Source	Link	Tags
Cisco IOS XR Software Authenticated User Privilege Escalation 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.

Legacy QID Mappings

316697 Cisco Internetwork Operating System (IOS) XR Software Authenticated User Privilege Escalation Vulnerability (cisco-sa-iosxr-LJtNFjeN)

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](#).

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