



CVE-2023-20135

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

Summary

CVE	CVE-2023-20135
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-13 17:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in Cisco IOS XR Software image verification checks could allow an authenticated, local attacker to execute a

Risk And Classification

Problem Types: CWE-367

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Cisco IOS XR Software Image Verification Vulnerability	MISC	sec.cloudapps.cisco.com	
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

317354 Cisco Internetwork Operating System (IOS) XR Software Image Verification Vulnerability (cisco-sa-Int-L9zOkBz5)

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