



CVE-2021-1623

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

Summary

CVE	CVE-2021-1623
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-23 03:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	A vulnerability in the Simple Network Management Protocol (SNMP) punt handling function of Cisco cBR-8 Converged Bro

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Cbr-8	-	All	All	All
Operating System	Cisco	ios Xe	All	All	All	All

References

Reference

- Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers Simple Network Management Protocol Denial of Service Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[317054](#) Cisco Internetwork Operating System (IOS) XE Software for Cisco cBR-8 Converged Broadband Routers Simple Network Management Protocol Denial of Service (DoS) Vulnerability (cisco-sa-cbr8snmp-zGjkZ9Fc)

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](#)