



CVE-2022-20714

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

Summary

CVE	CVE-2022-20714
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-15 15:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	A vulnerability in the data plane microcode of Lightspeed-Plus line cards for Cisco ASR 9000 Series Aggregation Services F

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 9902	-	All	All	All
Hardware	Cisco	Asr 9903	-	All	All	All
Operating System	Cisco	ios Xr	-	All	All	All

References

Reference	Source	Link
20220413 Cisco IOS XR Software for ASR 9000 Series Routers Lightspeed-Plus Line Cards Denial of Service Vulnerability	CISCO	toc
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[317177](#) Cisco Internetwork Operating System (IOS) XR Software for ASR 9000 Series Routers Lightspeed-Plus Line Cards Denial of Service (DoS)Vulnerability (cisco-sa-lsplus-Z6AQEOjk)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)