



CVE-2023-20126

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

Summary

CVE	CVE-2023-20126
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-04 20:15:00 UTC
Updated	2023-11-07 04:06:00 UTC
Description	A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated user to execute arbitrary code on the device.

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Spa112	-	All	All	All
Operating System	Cisco	Spa112 Firmware	1.4.1	sr9	All	All

References

Reference	Source	Link	Tags
Cisco SPA112 2-Port Phone Adapters Remote Command Execution Vulnerability	CISCO	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

[730795](#) Cisco SPA112 2-Port Phone Adapters Remote Command Execution Vulnerability (cisco-sa-spa-unauth-upgrade-UqhyTWW)

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](#)