CVE-2022-20784

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-20784
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-06 18:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	A vulnerability in the Web-Based Reputation Score (WBRS) engine of Cisco AsyncOS Software for Cisco Web Security App

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Web Security Appliance	-	All	All	All
Application	Cisco	Web Security Appliance	All	All	All	All

References

Reference	Source	Link	Tags
20220406 Cisco Web Security Appliance Filter Bypass Vulnerability	CISCO	tools.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

317141 Cisco Web Security Appliance Filter Bypass Vulnerability (cisco-sa-swa-filter-bypass-XXXTU3X)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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