CVE-2022-20737

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-20737
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-03 04:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	A vulnerability in the handler for HTTP authentication for resources accessed through the Clientless SSL VPN portal of Cisc

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All

References

Reference	Source	Link	Tag
20220427 Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317184 Cisco Adaptive Security Appliance (ASA) Clientless Secure Sockets Layer (SSL) Virtual Private Network (VPN) Heap Overflow Vulnerability (cisco-sa-asa-ssl-vpn-heap-zLX3FdX)

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