CVE-2009-4455

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-4455
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-29 23:30:00 UTC
Updated	2018-10-10 19:49:00 UTC
Description	The default configuration of Cisco ASA 5500 Series Adaptive Security Appliance (Cisco ASA) 7.0, 7.1, 7.2, 8.0, 8.1, and 8.2

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Adaptive Security Appliance 5500	7.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.2	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.2	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	7.2	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.0	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.1	All	All	All
Hardware	Cisco	Adaptive Security Appliance 5500	8.2	All	All	All

References

Reference	Source	Link
61132	OSVDB	osvdb.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.v

Alert Details - Security Center - Cisco Systems	CONFIRM	tools.c
SecurityFocus	BUGTRAQ	www.s
Cisco ASA WebVPN Bookmark URLs Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secuni
Cisco ASA WebVPN Bookmark List Can Be Bypassed By Remote Authenticated Users - SecurityTracker	SECTRACK	www.s
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**