CVE-2009-1220

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

Summary

CVE	CVE-2009-1220
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-01 18:30:00 UTC
Updated	2018-10-10 19:35:00 UTC
Description	Cross-site scripting (XSS) vulnerability in +webvpn+/index.html in WebVPN on the Cisco Adaptive Security Appliances (AS

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Adaptive Security Appliance	5520	All	All	All
Hardware	Cisco	Adaptive Security Appliance	5520	All	All	All
Operating System	Cisco	Ios	7.2(2)22	All	All	All
Operating System	Cisco	Ios	7.2\(2\)22	All	All	All
Operating System	Cisco	Ios	7.2\(2\)22	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FULLDISC	archi
SecurityFocus	BUGTRAQ	www.
Cisco ASA Appliance WebVPN Cross Site Scripting Vulnerability	BID	www.
SecurityFocus	BUGTRAQ	www.
IBM X-Force Exchange	XF	excha
Cisco ASA Input Validation Flaw in Clientless SSL VPN Feature Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.
Alert Details - Security Center - Cisco Systems	CONFIRM	tools.
CVE Program record	CVE.ORG	www.

NVD vulnerability detail NVD nvd.n

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**