CVE-2017-6764

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

Summary

CVE	CVE-2017-6764
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 06:29:00 UTC
Updated	2023-08-11 18:54:00 UTC
Description	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) 9.5(1) could allow an a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Adaptive Security Appliance Software	9.5(1)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.5\(1\)	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	9.5\(1\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.5\(1\)	All	All	All

References

Reference	Source	Link
Cisco Adaptive Security Appliance CVE-2017-6764 Cross Site Scripting Vulnerability	BID	www.securityfo
Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability	CONFIRM	tools.cisco.con
Cisco ASA Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.securitytr
Cisco Bug: CSCvd82064 - Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability	CONFIRM	quickview.clou
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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