



CVE-2017-12265

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-12265
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-05 07:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an

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	-	All	All	All
Application	Cisco	Adaptive Security Appliance	-	All	All	All

References

Reference	Source	Lin
Cisco ASA Input Validation Flaw in WEBVPN Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTrack	ww
Cisco Adaptive Security Appliance Software HREF Cross-Site Scripting Vulnerability	CONFIRM	too
Cisco Adaptive Security Appliance Software CVE-2017-12265 Cross Site Scripting Vulnerability	BID	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

Free CVE JSON API cve.report/api

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