CVE-2015-0732

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

Summary

CVE	CVE-2015-0732
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-29 01:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in Cisco AsyncOS on the Web Security Appliance (WSA) 9.0.0-193; Email Security A

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Content Security Management Virtual Appliance	9.1.0-033	All	All	All

Operating System	Cisco	Email Security Appliance Firmware	8.5.6-113	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	9.1.0-032	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	9.1.1-000	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	9.6.0-000	All	All	All
Application	Cisco	Web Security Appliance	9.0.0-193	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Cisco Email Security Appliance AsyncOS Cross-Site Scripting Vulnerability	af854a3a-2127-4
Cisco Email Security Appliance Input Validation Flaw Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	af854a3a-2127-4
Cisco Web Security Appliance Input Validation Flaw Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	af854a3a-2127-4
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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