CVE-2018-0093

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

Summary

CVE	CVE-2018-0093
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-18 06:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the web-based management interface of Cisco Web Security Appliance (WSA) could allow an unauthentic

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Web Security Appliance	All	All	All	All
Application	Cisco	Web Security Appliance	All	All	All	All

References

Reference	Source
Cisco Web Security Appliance Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRACK
Cisco Web Security Appliance Reflected Cross-Site Scripting Vulnerability	CONFIRM
Cisco Web Security Appliance CVE-2018-0093 Cross Site Scripting Vulnerability	BID
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.

Free CVE JSON API cve.report/api

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