CVE-2020-3117

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-3117
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-23 01:15:00 UTC
Updated	2020-10-01 15:37:00 UTC
Description	A vulnerability in the API Framework of Cisco AsyncOS for Cisco Web Security Appliance (WSA) and Cisco Content Securi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Content Security Management Appliance	All	All	All	All
Application	Cisco	Content Security Management Appliance	All	All	All	All
Application	Cisco	Web Security Appliance	11.8.0-382	All	All	All
Application	Cisco	Web Security Appliance	12.0.1-268	All	All	All
Application	Cisco	Web Security Appliance	11.8.0-382	All	All	All
Application	Cisco	Web Security Appliance	12.0.1-268	All	All	All

References

Reference	Source	Link
Cisco Web Security Appliance and Cisco Content Security Management Appliance HTTP Header Injection Vulnerability	CISCO	tools.c
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

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