CVE-2017-12303

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

Summary

CVE	CVE-2017-12303
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-16 07:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the Advanced Malware Protection (AMP) file filtering feature of Cisco AsyncOS Software for Cisco Web Se

Risk And Classification

Problem Types: CWE-358

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Asyncos	10.1.1-234	All	All	All
Operating System	Cisco	Asyncos	10.1.1-235	All	All	All
Operating System	Cisco	Asyncos	10.1.1-234	All	All	All
Operating System	Cisco	Asyncos	10.1.1-235	All	All	All

References

Reference
Cisco Web Security Appliance Advanced Malware Protection File Bypass Vulnerability
Cisco Web Security Appliance CVE-2017-12303 Remote Security Bypass Vulnerability
Cisco Web Security Appliance File Hashing Error Lets Remote Users Bypass Advanced Malware Protection on the Target System - SecurityT
CVE Program record
NVD vulnerability detail

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