CVE-2018-0237

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0237
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-19 20:29:00 UTC
Updated	2020-09-04 18:26:00 UTC
Description	A vulnerability in the file type detection mechanism of the Cisco Advanced Malware Protection (AMP) for Endpoints macOS

Risk And Classification

Problem Types: CWE-706

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Advanced Malware Protection For Endpoints	1.4(5)	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	1.4\(5\)	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	1.4\(5\)	All	All	All

References

Reference	Source	Link
Cisco AMP for Endpoints macOS Connector DMG File Malware Bypass Vulnerability	CONFIRM	tools.cisco.com
Research: Auto-detection of Compressed Files in Apple's macOS | Nightwatch Cybersecurity	MISC	wwws.nightwatchcybersecurity.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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