



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	www.nightwatchcybersecurity.com
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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)