



CVE-2017-3800

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3800
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-26 07:59:00 UTC
Updated	2017-07-26 01:29:00 UTC
Description	A vulnerability in the content scanning engine of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) could

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Email Security Appliance	9.7.1-066	All	All	All
Application	Cisco	Email Security Appliance	9.7.1-hp2-207	All	All	All
Application	Cisco	Email Security Appliance	9.8.5-085	All	All	All
Application	Cisco	Email Security Appliance	9.7.1-066	All	All	All
Application	Cisco	Email Security Appliance	9.7.1-hp2-207	All	All	All
Application	Cisco	Email Security Appliance	9.8.5-085	All	All	All

References

Reference	Source	Link
Cisco Email Security Appliance for AsyncOS CVE-2017-3800 Remote Security Bypass Vulnerability	BID	www
Cisco Email Security Appliance Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker	SECTrack	www
Cisco Email Security Appliance Filter Bypass Vulnerability	CONFIRM	too
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

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