



CVE-2017-3818

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-3818
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-03 07:59:00 UTC
Updated	2017-07-25 01:29:00 UTC
Description	A vulnerability in the Multipurpose Internet Mail Extensions (MIME) scanner of Cisco AsyncOS Software for Cisco Email Se

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Email Security Appliance Firmware	9.7.1-066	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	9.7.1-066	All	All	All

References

Reference	
Cisco Email Security Appliance Malformed MIME Header Filtering Bypass Vulnerability	C
Cisco Email Security Appliance Bug in MIME Scanner Lets Remote Users Bypass Security Filters on the Target System - SecurityTracker	S
Cisco Email Security Appliance for AsyncOS CVE-2017-3818 Remote Security Bypass Vulnerability	E
CVE Program record	C
NVD vulnerability detail	N

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](#)