



CVE-2018-0419

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

Summary

CVE	CVE-2018-0419
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-15 20:29:00 UTC
Updated	2019-10-09 23:32:00 UTC
Description	A vulnerability in certain attachment detection mechanisms of Cisco Email Security Appliances (ESA) could allow an unauth

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	-	All	All	All
Application	Cisco	Email Security Appliance	-	All	All	All

References

Reference

- Cisco Email Security Appliance Executable File Detection Bug Lets Remote Users Bypass Security Filtering on the Target System - SecurityT
- Cisco Email Security Appliance EXE File Scanning Bypass Vulnerability
- Cisco Email Security Appliance EXE File Scanning CVE-2018-0419 Remote Security Bypass Vulnerability
- 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.

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](#)