

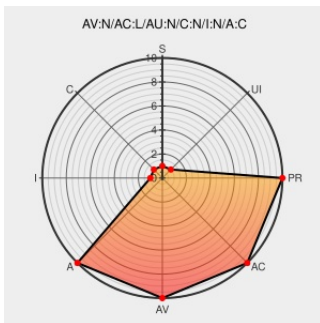


CVE-2015-6291

Published on: 11/05/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6291

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Email Security Appliance](#) from [Cisco](#) contain the following vulnerability:

Cisco AsyncOS before 8.5.7-043, 9.x before 9.1.1-023, and 9.5.x and 9.6.x before 9.6.0-046 on Email Security Appliance (ESA) devices mishandles malformed fields during body-contains, attachment-contains, every-attachment-contains, attachment-binary-contains, dictionary-match, and attachment-dictionary-match filtering, which

allows remote attackers to cause a denial of service (memory consumption) via a crafted attachment in an e-mail message, aka Bug ID CSCuv47151.

CVE-2015-6291 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Cisco Email Security Appliance Email Scanner Denial of Service Vulnerability

Tags

[Vendor Advisory](#)
[tools.cisco.com](#)
[text/html](#)

Link

[CISCO 20151104 Cisco Email Security Appliance Email Scanner Denial of Service Vulnerability](#)

Cisco Email Security Appliance Email Scanner Bug Lets Remote Users Consume Excessive Memory Resources - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1034064](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Email Security Appliance	7.7.0-000	All	All	All
Application	Cisco	Email Security Appliance	7.7.1-000	All	All	All
Application	Cisco	Email Security Appliance	8.0_base	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-052	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-073	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-074	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-106	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-113	All	All	All
Application	Cisco	Email Security Appliance	8.5.7-042	All	All	All
Application	Cisco	Email Security Appliance	8.5_base	All	All	All
Application	Cisco	Email Security Appliance	9.0.0	All	All	All
Application	Cisco	Email Security Appliance	9.0.0-212	All	All	All
Application	Cisco	Email Security Appliance	9.0.0-461	All	All	All
Application	Cisco	Email Security Appliance	9.0.5-000	All	All	All
Application	Cisco	Email Security Appliance	9.1.0-032	All	All	All
Application	Cisco	Email Security Appliance	9.6.0-042	All	All	All
Application	Cisco	Email Security Appliance	7.7.0-000	All	All	All
Application	Cisco	Email Security Appliance	7.7.1-000	All	All	All
Application	Cisco	Email Security Appliance	8.0_base	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-052	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-073	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-074	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-106	All	All	All
Application	Cisco	Email Security Appliance	8.5.6-113	All	All	All
Application	Cisco	Email Security Appliance	8.5.7-042	All	All	All
Application	Cisco	Email Security Appliance	8.5_base	All	All	All
Application	Cisco	Email Security Appliance	9.0.0	All	All	All
Application	Cisco	Email Security Appliance	9.0.0-212	All	All	All
Application	Cisco	Email Security Appliance	9.0.0-461	All	All	All
Application	Cisco	Email Security Appliance	9.0.5-000	All	All	All
Application	Cisco	Email Security Appliance	9.1.0-032	All	All	All

Application	Cisco	Email Security Appliance	9.1.0-032	All	All	All
Application	Cisco	Email Security Appliance	9.6.0-042	All	All	All
cpe:2.3:a:cisco:email_security_appliance:7.7.0-000:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:7.7.1-000:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.0_base:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-052:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-073:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-074:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-106:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-113:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.7-042:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5_base:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.0.0:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.0.0-461:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.1.0-032:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.6.0-042:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:7.7.0-000:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:7.7.1-000:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.0_base:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-052:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-073:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-074:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-106:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.6-113:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5.7-042:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:8.5_base:*****:.*:						
cpe:2.3:a:cisco:email_security_appliance:9.0.0:*****:.*:						

cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-461:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-032:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.6.0-042:*:*:*:*:*:

cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-461:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-032:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.6.0-042:*:*:*:*:*:

cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-461:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-032:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.6.0-042:*:*:*:*:*:

cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-461:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-032:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.6.0-042:*:*:*:*:*:

cpe:2.3:a:cisco:email_security_appliance:9.0.0-212:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.0-461:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.0.5-000:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.1.0-032:*:*:*:*:*:
cpe:2.3:a:cisco:email_security_appliance:9.6.0-042:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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](#).

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