

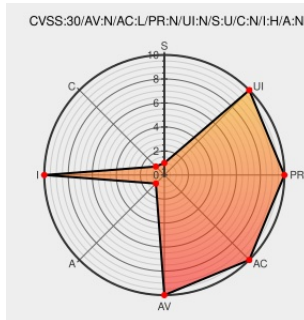


# CVE-2016-6458

Published on: 11/18/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:11 PM UTC

## CVE-2016-6458

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

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

A vulnerability in the content filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to bypass content filters configured on an affected device. Email that should have been filtered could instead be forwarded by the device. This vulnerability affects all

releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to use a content filter for email attachments that are protected or encrypted. More Information: CSCva52546. Known Affected Releases: 10.0.0-125 9.7.1-066.

CVE-2016-6458 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

CVE References

| Description                                                                                                 | Tags                                                                                                                 | Link                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Email Security Appliance Lets Remote Users Bypass RAR Scanning on the Target System - SecurityTracker | <a href="http://www.securitytracker.com">www.securitytracker.com</a><br><a href="#">text/html</a>                    |  <a href="#">SECTrack 1037182</a>                                                                                                                                                                                        |
| Cisco AsyncOS CVE-2016-6458 Remote Security Bypass Vulnerability                                            | <a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                                                    |  <a href="#">BID 94074</a>                                                                                                                                                                                               |
| Cisco Email Security Appliance RAR File Attachment Scanner Bypass Vulnerability                             | <a href="#">Vendor Advisory</a><br><a href="http://tools.cisco.com">tools.cisco.com</a><br><a href="#">text/html</a> |  <a href="#">CONFIRM</a><br><a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-esa">tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-esa</a> |

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](mailto: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 |
|------------------|-----------------------|---------------------------------------------------|------------|--------|---------|----------|
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 10.0.0-124 | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 10.0.0-125 | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.1-066  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.2-046  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.2-047  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.2-054  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.9.6-026  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.9_base   | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 10.0.0-124 | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 10.0.0-125 | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.1-066  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.2-046  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.2-047  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">Email Security Appliance Firmware</a> | 9.7.2-054  | All    | All     | All      |

|                                                                     |       |                                   |           |           |     |     |
|---------------------------------------------------------------------|-------|-----------------------------------|-----------|-----------|-----|-----|
| System                                                              |       |                                   |           |           |     |     |
| Operating System                                                    | Cisco | Email Security Appliance Firmware | 9.9.6-026 | All       | All | All |
| Operating System                                                    | Cisco | Email Security Appliance Firmware | 9.9_base  | All       | All | All |
| cpe:2.3:o:cisco:email_security_appliance_firmware:10.0.0-124:*****: |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:10.0.0-125:*****: |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.1-066:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.2-046:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.2-047:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.2-054:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.9.6-026:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.9_base:*****:   |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:10.0.0-124:*****: |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:10.0.0-125:*****: |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.1-066:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.2-046:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.2-047:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.2-054:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.9.6-026:*****:  |       |                                   |           |           |     |     |
| cpe:2.3:o:cisco:email_security_appliance_firmware:9.9_base:*****:   |       |                                   |           |           |     |     |
| No vendor comments have been submitted for this CVE                 |       |                                   |           |           |     |     |
| ← Previous ID                                                       |       |                                   |           | Next ID → |     |     |