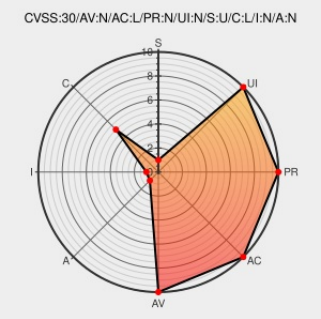
# CVE-2016-6463

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

Last Modified on: 03/23/2021 11:27:12 PM UTC

## CVE-2016-6463

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 email filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to bypass Advanced Malware Protection (AMP) filters that are configured for an affected device. This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for both virtual and hardware versions of Cisco Email Security Appliances, if the AMP feature is configured to scan incoming email attachments. More Information: CSCuz85823. Known Affected Releases: 10.0.0-082 9.7.0-125 9.7.1-066. Known Fixed Releases: 10.0.0-203 9.7.2-131.

CVE-2016-6463 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.3 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | LOW | NONE | NONE |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Cisco Email Security Appliance MIME Header Processing Filter Bypass Vulnerability | Vendor Advisory<br>tools.cisco.com<br>text/html | CONFIRM<br>tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161116-esa2 |
| Cisco AsyncOS CVE-2016-6463 Remote Security Bypass Vulnerability | cve.report (archive)<br>text/html | BID 94363 |

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 |
|---|---|---|---|---|---|---|
| Operating System | Cisco | Email Security Appliance Firmware | 10.0.0-082 | All | All | All |
| Operating System | Cisco | Email Security Appliance Firmware | 9.7.0-125 | All | All | All |
| Operating System | Cisco | Email Security Appliance Firmware | 9.7.1-06 | All | All | All |
| Operating System | Cisco | Email Security Appliance Firmware | 10.0.0-082 | All | All | All |
| Operating System | Cisco | Email Security Appliance Firmware | 9.7.0-125 | All | All | All |
| Operating System | Cisco | Email Security Appliance Firmware | 9.7.1-06 | All | All | All |

cpe:2.3:o:cisco:email_security_appliance_firmware:10.0.0-082:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.0-125:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.1-06:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:email_security_appliance_firmware:10.0.0-082:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.0-125:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:email_security_appliance_firmware:9.7.1-06:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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