# Advanced Notification of a Vulnerability in Cisco ASA Software

CERT ae Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

| | | | | |
|---|---|---|---|---|
| **Security Advisory** | ADV-19-01 | **Criticality** | High |  |
| **Advisory Released On** | 16 January 2019 | | | |

**Impact**

A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) lead to a denial of service (DoS) on impacted devices and can be exploited by a remote and unauthenticated attacker who simply sends an email.

**Solution**

Adhere the advice written in the solution section.

**Affected Platforms**

Cisco AsyncOS Software for Cisco ESAs.

## Summary

A vulnerability in email message filtering which contain sources of whitelisted URLs. This vulnerability allow an unauthenticated, remote attacker to cause the CPU utilization to increase to 100 percent, causing a denial of service (DoS) condition on an affected device. Software updates have been released by Cisco to fix this problem. There are workarounds that address this vulnerability.

## Threat Details

This vulnerability affects all software versions prior to the first fixed release of Cisco AsyncOS Software for Cisco ESAs, both virtual and hardware, if the URL Filtering as Global Setting feature is enabled and a URL whitelist is in use. By default, the URL Filtering as Global Setting feature is disabled.

To determine whether a vulnerable release of Cisco AsyncOS Software is running on an ESA, administrators can use the version command in the ESA CLI.

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following products:

- Content Security Management Appliance, virtual and hardware versions
- Web Security Appliance, virtual and hardware versions

## Solution

Cisco has released free software updates that address the vulnerability described in this advisory.

In the following table, the left column lists major releases of Cisco AsyncOS Software for ESA. The right column indicates whether a major release is affected by the vulnerability described in this advisory and the first minor release that includes the fix for this vulnerability.

Customers should upgrade to an appropriate release as indicated in the following table:

| Cisco AsyncOS Software for ESA Major Release | First Fixed Release for This Vulnerability |
|---|---|
| Prior to 9.0 | Affected; Migrate to 11.0.2-044 MD |
| 9.x | Affected; Migrate to 11.0.2-044 MD |
| 10.x | Affected; Migrate to 11.0.2-044 MD |
| 11.0.x | 11.0.2-044 MD1 |
| 11.1.x | 11.1.2-023 MD2 |
| 12.x | Not affected |

1: 11.0.2-044 will run on all legacy hardware for ESA models x70, x80, x90 and the virtual appliances.

2: 11.1.2-023 will run on ESA models x80, x90 and the virtual appliances.

## References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190109-esa-url-dos

## Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae