CERT-EU Security Advisory 2018-004

Critical Vulnerability in Cisco Adaptive Security Appliance

February 6, 2018 — v1.1

History:

- *31/01/2018 — v1.0: Initial publication*
- *06/01/2018 — v1.1: Corrections after CISCO updated advisory*

Summary

On the 29nd of January 2018, CISCO published a security advisory for a remote code execution and denial of service vulnerability affecting Cisco Adaptive Security Appliance (ASA) [1]. The vulnerability is located in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software and could allow an unauthenticated, remote attacker to cause a reboot of the affected system or to remotely execute code.

On the 5th of February 2018, CISCO updated the advisory after identifying additional attack vectors and release of new patches.

Technical Details

The vulnerability received the following CVE: CVE-2018-0101 [2].

The vulnerability is due to an attempt to *double free* a region of memory when the `webvpn` feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a `webvpn`-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, or cause a reboot of the affected device.

To determine whether `webvpn` is enabled for at least one interface, administrators can use the `show running-config webvpn` command at the CLI and verify that the command returns at least one enable `<if_name>` line:

```
ciscoasa# show running-config webvpn
webvpn
enable Outside
```

Administrators can also use the `show asp table socket command` and look for an `SSL` and a `DTLS` listen socket on `TCP port 443`:

```
ciscoasa# show asp table socket
Protocol  Socket    State      Local Address       Foreign Address
SSL       00005898  LISTEN     10.48.66.202:8443    0.0.0.0:*
TCP       00009718  LISTEN     10.48.66.202:23      0.0.0.0:*
TCP       0000e708  LISTEN     10.48.66.202:22      0.0.0.0:*
SSL       00011cc8  LISTEN     10.48.66.202:443     0.0.0.0:*
DTLS      000172f8  LISTEN     10.48.66.202:443     0.0.0.0:*
```

To determine whether a vulnerable version of Cisco ASA Software is running on a device, administrators can use the `show version` command in the CLI:

```
ciscoasa# show version | include Version
Cisco Adaptive Security Appliance Software Version 9.2(1)
Device Manager Version 7.4(1)
```

This vulnerability also applies to the FTD 6.2.2 software release. Administrators can use the `show version` command at the CLI to determine the FTD release:

```
show version
----------------------[ ftd ]----------------------
Model : Cisco ASA5525-X Threat Defense (75) Version 6.2.2 (Build 362)
UUID : 2849ba3c-ecb8-11e6-98ca-b9fc2975893c
Rules update version : 2017-03-15-001-vrt
VDB version : 279
---------------------------------------------------
```

Products Affected

The following products are affected if they are running a vulnerable version of CISCO ASA with the webvpn feature is enabled:

- 3000 Series Industrial Security Appliance (ISA)
- ASA 5500 Series Adaptive Security Appliances
- ASA 5500-X Series Next-Generation Firewalls
- ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- ASA 1000V Cloud Firewall
- Adaptive Security Virtual Appliance (ASAv)
- Firepower 2100 Series Security Appliance
- Firepower 4110 Security Appliance
- Firepower 9300 ASA Security Module
- Firepower Threat Defense Software (FTD)

The impacted versions of CISCO ASA are:

- 8.x (all versions)
- 9.0 (all versions)
- 9.1 prior to 9.1.7.23
- 9.2 prior to 9.2.4.27
- 9.3 (all versions)
- 9.4 prior to 9.4.4.16
- 9.5 (all versions)

- 9.6 prior to 9.6.4.3
- 9.7 prior to 9.7.1.21
- 9.8 prior to 9.8.2.20
- 9.9 prior to 9.9.1.2

The impacted version of FTD Software are:

- 6.0.0
- 6.0.1
- 6.1.0
- 6.2.0
- 6.2.1
- 6.2.2

Recommendations

For CISCO ASA, update to release not affected by the vulnerability. If using version 8.x, 9.0, 9.3 or 9.5, you need to migrate to higher CISCO ASA major release.

For FTD software, apply the provided hotfixes [3]. For version 6.0.0 and 6.2.1, you also need to migrate to higher FTD software version.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0101

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1#fixed