Security Advisory 2024-043

Vulnerabilities in Cisco ASA and FTD Software

April 24, 2024 — v1.0

TLP:CLEAR

History:

- *24/04/2024 — v1.0 – Initial publication*

Summary

On April 24, 2024, Cisco disclosed three vulnerabilities in its management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software product.

Some of these vulnerabilities are currently being exploited[1]. It is recommended upgrading affected products as soon as possible, and checking for possible compromise.

Technical Details

The vulnerability **CVE-2024-20353** [1], with a CVSS score of 8.6, allows an attacker to cause a DoS condition by sending a crafted HTTP request to the web server on a targeted device. A successful exploit would result in an unexpected reloading of the device. This vulnerability is due to incomplete error checking when parsing an HTTP header.

The vulnerability **CVE-2024-20359** [2], with a CVSS score of 6.0, allows an authenticated, local attacker to execute arbitrary code with root-level privileges on the affected device by copying a crafted file to its `disk0:` file system. The execution occurs after the next reload of the targeted device. This vulnerability is due to improper validation of a file when it is read from system flash memory. It is also important to note that the injected code could persist across device reboots. Administrator-level privileges are required to exploit this vulnerability.

The vulnerability **CVE-2024-20358** [3], with a CVSS score of 6.0, allows an authenticated, local attacker to execute arbitrary commands on the underlying operating system (i.e., Linux) with root-level privileges. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. This vulnerability exists because the contents of a backup file are improperly sanitised at restore time. Administrator-level privileges are required to exploit this vulnerability.

Affected Products

These vulnerabilities affect Cisco ASA and FTD appliances. In order to understand if one version is affected, Cisco provides its Cisco Software Checker tool.

CVE-2024-20353

This vulnerability affects Cisco ASA Software and FTD Software if they have one or more of the vulnerable configurations listed below

To determine whether a device that is running Cisco ASA Software or FTD Software is affected, use the `show asp table socket | include SSL` command and look for an SSL listen socket on any TCP port. If a socket is present in the output, the device should be considered vulnerable. The following example shows the output for a Cisco ASA device with two SSL listen sockets on TCP port 443 and TCP port 8443:

```
ciscoasa#  show asp table socket | include SSL
SSL       00185038  LISTEN     172.16.0.250:443    0.0.0.0:*
SSL       00188638  LISTEN      10.0.0.250:8443    0.0.0.0:*
```

ASA Software Vulnerable Configuration

In the following table, the left column lists Cisco ASA Software features that are potentially vulnerable. The right column indicates the basic configuration for the feature from the `show running-config` CLI command, if it can be determined. These features could cause the SSL listen sockets to be enabled.

Cisco ASA Software Feature	Possible Vulnerable Configuration
AnyConnect IKEv2 Remote Access (with client services)	crypto ikev2 enable [. . .] client-services port
Local Certificate Authority (CA)	crypto ca server \ no shutdown
Management Web Server Access (including ASDM and CSM)	http server enable \ http
Mobile User Security (MUS)	webvpn \ mus password \ mus server enable port \ mus
REST API	rest-api image disk0:/rest-api agent
SSL VPN	webvpn \ enable

Note: `Management Web Server Access` *and* `REST API` *would only be vulnerable from an IP address in the configured http command range.*

FTD Software Vulnerable Configuration

In the following table, the left column lists Cisco FTD Software features that are potentially vulnerable. The right column indicates the basic configuration for the feature from the `show running-config` CLI command, if it can be determined. These features could cause the SSL listen sockets to be enabled.

Cisco FTD Software Feature	Possible Vulnerable Configuration
AnyConnect IKEv2 Remote Access (with client services)	crypto ikev2 enable [. . .] client-services port

Cisco FTD Software Feature	Possible Vulnerable Configuration
AnyConnect SSL VPN	webvpn enable
HTTP server enabled	http server enable http

CVE-2024-20358

Cisco FTD Software is affected only when lockdown mode has been enabled to restrict Linux shell access. Lockdown mode is disabled by default.

Recommendations

CERT-EU recommends updating to the latest version of Cisco Adaptive Security Appliance (ASA) Software and/or Cisco Firepower Threat Defense (FTD) Software product as soon as possible to mitigate these vulnerabilities.

CERT-EU also recommends following the compromise assessment steps to ensure that vulnerable devices have not been exploited.

Compromise assessment

Cisco Talos has released a blog post to explain how some of these vulnerabilities have been found to be exploited [1].

1. First, organisations should look for any flows to/from ASA devices to any of the IP addresses present in the IOC list provided at the bottom of this blog. This is one indication that further investigation is necessary.
2. Additionally, organisations can issue the command `show memory region | include lina` to identify another indicator of compromise. If the output indicates more than one executable memory region (memory regions having `r-xp` permissions), especially if one of these memory sections is exactly 0x1000 bytes, then this is a sign of potential tampering.
3. It is also recommended, even in the absence of more than one executable memory region, to follow the "Forensic Recovery and Identification of Line Runner" steps provided in the blog post.

References

[1] https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

[4] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm