Smarttech
YOUR 24/7 SECURITY PARTNER

Threat Report

Zero-Day Vulnerabilities Discovered in Cisco ASA and FTD 25th April 2024

NSAI

QUALITY
I.S. EN ISO 27001:2013
NSAI Certified

QUALITY
I.S. EN ISO 9001:2015
NSAI Certified

Document ID	SMA - Threat Report
Document status	ISSUED
Issue Number	02
Authors	Razvan Constantin <razvan.constantin@smarttech.com >
Verified by	Alin Curcan <alin.curcan@smarttech247.com>
Last modified	2024-04-25
Issue Date	2024-04-25

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Three vulnerabilities have been discovered in Cisco ASA and FTD.
The cybercriminals, identified as UAT4356 by Cisco Talos and STORM-1849 by Microsoft, initiated their attack on vulnerable edge devices in November 2023 as part of a cyber-espionage campaign named ArcaneDoor. Although Cisco hasn't determined the initial attack vector, they have addressed and patched two vulnerabilities—CVE-2024-20353, causing denial of service, and CVE-2024-20359, allowing persistent local code execution—that were leveraged as zero-days in these attacks. Cisco first became aware of the ArcaneDoor campaign in January 2024 and discovered evidence suggesting the attackers had been developing and testing exploits for these zero-days since at least July 2023.

RISK

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

TECHNICAL SUMMARY

More details related to these vulnerabilities are as follows:

CVE ID	Description
CVE-2024-20358 (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability) CVSS Base Score: 6.0	• A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.

	• This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.
CVE-2024-20359 (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability) CVSS Base Score: 6.0	• A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. • This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.
CVE-2024-20353 (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability) CVSS Base Score: 8.6	• A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. • This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit

	could allow the attacker to cause a DoS condition when the device reloads.

Note: *VPR Score is not available at this moment*

Affected Products:

- **CVE-2024-20358** (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability)
  - At the time of publication, this vulnerability affected Cisco products if they were running a vulnerable release of Cisco ASA Software or FTD Software. No specific configuration is required.
  - Note: Cisco FTD Software is affected only when lockdown mode has been enabled to restrict Linux shell access. Lockdown mode is disabled by default. When lockdown mode is disabled, Linux shell access, including root-level shell access, is readily available through the expert CLI command on devices that are running Cisco FTD Software. For more information on lockdown mode, see the Cisco Secure Firewall Threat Defense Hardening Guide.
  - For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

- **CVE-2024-20359** (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability)
  - This vulnerability affects Cisco products if they are running a vulnerable release of Cisco ASA Software or FTD Software. No specific configuration is required.

- Recommendations:
  After upgrading to a release with the fix for this vulnerability, Cisco recommends that customers check the output of the **dir disk0:** command on the device CLI for any new *.zip* files that were not showing up before the upgrade.

If a new file named *client_bundle_install.zip* or any other unusual *.zip* file appears after the upgrade, copy that file off the device using the **copy** command and contact psirt@cisco.com referencing CVE-2024-20359. Include the outputs of the **dir disk0:** and **show version** commands from the device and the *.zip* file that was extracted from the device.

- **CVE-2024-20353** (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability)
  This vulnerability affects Cisco ASA Software and FTD Software if they have one or more of the vulnerable configurations listed in the following two tables. For more recommendation about the Fixed Software please check the Fixed Software section:

  - Determine Whether an ASA or FTD Device Is Affected

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)[1]	crypto ca server no shutdown
Management Web Server Access (including ASDM and CSM)[2]	http server enable http
Mobile User Security (MUS)	webvpn mus password mus server enable port mus
REST API[3]	rest-api image disk0:/rest-api agent
SSL VPN	webvpn enable

  - 1. In Cisco ASA Software Release 9.13 and later, Local CA is deprecated and has been removed.
  - 2. Management Web Server Access would only be vulnerable from an IP address in the configured http command range.
  - 3. REST API is vulnerable only 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)[1,2]	crypto ikev2 enable [...] client-services port
AnyConnect SSL VPN[1,2]	webvpn enable

HTTP server enabled[3]	http server enable http

- 1. Remote access VPN features are enabled from Devices > VPN > Remote Access in Cisco Firepower Management Center (FMC) Software or from Device > Remote Access VPN in Cisco Firepower Device Manager (FDM).
- 2. Remote access VPN features are first supported as of Cisco FTD Software Release 6.2.2.
- 3. The HTTP feature is enabled from Firepower Threat Defense Platform Settings > HTTP in the Cisco FMC Console.

Products Confirmed Not Vulnerable:

- **CVE-2024-20358** (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability)
  - Cisco has confirmed that this vulnerability does not affect Cisco Firepower Management Center (FMC) Software.

- **CVE-2024-20359** (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability)
  - Cisco has confirmed that this vulnerability does not affect Cisco Firepower Management Center (FMC) Software.

- **CVE-2024-20353** (Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability)
  - Cisco has confirmed that this vulnerability does not affect Cisco FMC Software.

Recommendations

Smarttech247 team recommends the following actions to be taken:

1. **Upgrade** to the latest versions in order to obtain a fix for these vulnerabilities. Please check the Fixed releases for the respective version details.

2. **Upgrade** software and operating systems, applications, and firmware on network assets in a timely manner for prevention.

3. **Use** the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.

4. **Apply** the Principle of Least Privilege to all systems and services.

5. **Apply** advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.

6. **Kindly** ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2
- https://www.bleepingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/
- https://nvd.nist.gov/vuln/detail/CVE-2024-20358
- https://nvd.nist.gov/vuln/detail/CVE-2024-20359
- https://nvd.nist.gov/vuln/detail/CVE-2024-20353

List of CVEs

- CVE-2024-20358
- CVE-2024-20359
- CVE-2024-20353