National Cyber Security Centre

2404260154-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Vulnerabilities in Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) (CVE-2024-2035, CVE-2024-20358, CVE-2024-20359)

Friday 26th April, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

Published: 2024-04-24T19:15:00
Vendor: Cisco
Products: Cisco Adaptive Security Appliance (ASA) software and Firepower Threat Defense (FTD) software
CVE IDs: CVE-2024-20353, CVE-2024-20358, CVE-2024-20359
EPSS[1]**:**

- CVE-2024-20353 (0.85)
- CVE-2024-20358 (0.09)
- CVE-2024-20359 (0.85)

Summary: Cisco has disclosed vulnerabilities impacting its ASA and FTD devices, with ongoing attacks reported by its Product Security Incident Response Team (PSIRT). These vulnerabilities enable malware implantation, command execution, and potential data exfiltration. Notably, CVE-2024-20353 and CVE-2024-20359 are being **actively exploited**.

Products Affected

At the time of publication, these vulnerabilities affect Cisco products if they are running a vulnerable release of Cisco ASA or FTD software. Cisco FTD software is affected only when lockdown mode has been enabled to restrict Linux shell access. Lockdown mode is disabled by default.

Impact

CVE-2024-20353 (CVSS 8.6): A vulnerability in the management and VPN web servers for Cisco ASA software and FTD software could allow an unauthenticated remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.

CVE-2024-20358 (CVSS 6.0): A vulnerability in the ASA restore functionality available in ASA software and Firepower 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.

CVE-2024-20359 (CVSS 6.0): A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins which has been available in ASA software and 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.

[1] https://www.first.org/epss/articles/prob_percentile_bins

Indicators of Compromise

The Canadian Centre for Cyber Security (Cyber Centre), Australian Signals Directorate's Australian Cyber Security Centre and the UK NCSC have observed the following malicious IP addresses targeting networks. The below can be considered high confidence indicators of malicious activity and organisations are reminded not to probe the provided IP addresses, but instead to check historical network logs, specifically for large volumes of data being transferred. Particular attention should be given if these IP addresses were observed through **December 2023 to February 2024**:

IP Addresses
185.244.210[.]65
5.183.95[.]95
213.156.138[.]77
45.77.54[.]14
45.77.52[.]253
45.63.119[.]131
194.32.78[.]183
185.244.210[.]120
216.238.81[.]149
216.238.85[.]220
216.238.74[.]95
45.128.134[.]189
176.31.18[.]153
216.238.72[.]201
216.238.71[.]49
216.238.66[.]251
216.238.86[.]24
216.238.75[.]155
154.39.142[.]47
139.162.135[.]12

Recommendations

The NCSC strongly advises affected organisations to review their network logs for the listed IOCs and install the latest software updates from Cisco. There are no workarounds that address these vulnerabilities.

Additionally, organisations should 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 new files are found on the device, copy that file off the device using the copy command and contact certreport@ncsc.gov.ie.

Cisco's recommendations and mitigation's for the CVEs can be found in the respective links below:

- Cisco Security Advisory for CVE-2024-20353
- Cisco Security Advisory for CVE-2024-20358

- Cisco Security Advisory for CVE-2024-20359

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie