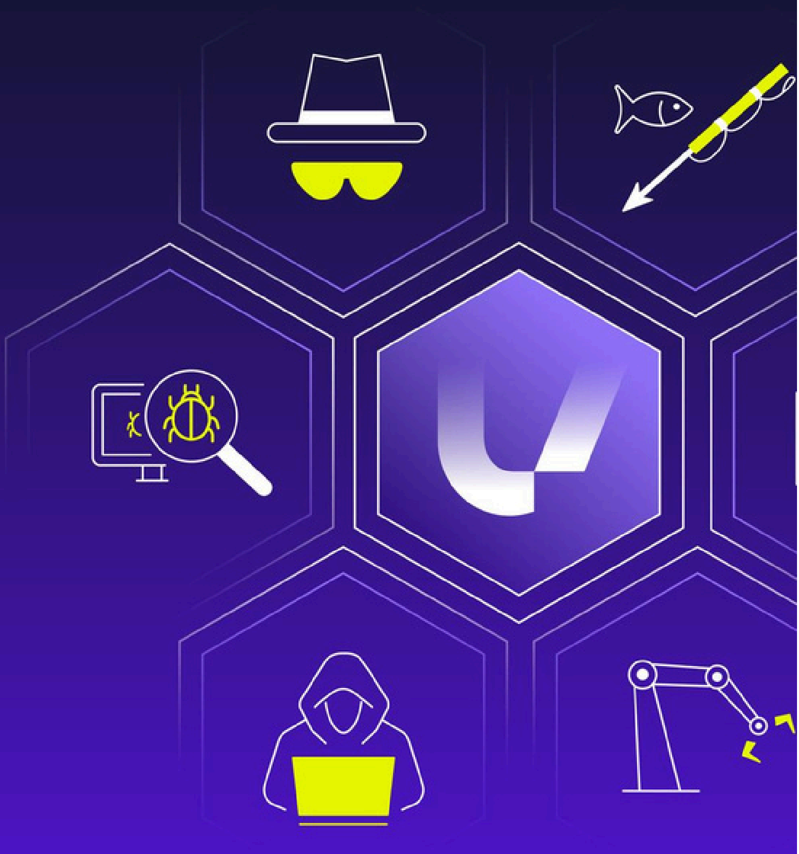
CONFIDENTIAL

THREAT REPORT:

Three New CVEs For CISCO ASA And FTD Software



Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
4/25/2024

Doc ID: ECORP_SUM_07032023_v1.1

Contents

1 Executive Summary

The Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on April 24, 2024, regarding actively exploited vulnerabilities within Cisco's ASA and FTD software. A new Advanced Persistent Threat (APT) group classified as UAT4356 by Talos and STORM-1849 by the Microsoft Threat Intelligence Center was also nicknamed "ArcaneDoor" by researchers earlier this year. ArcaneDoor could take control of a Cisco ASA or FTD system by exploiting three new CVEs: CVE-2024-20353 (CVSS score 8.6), CVE-2024-20359 (CVSS score 6.0), and CVE-2024-20358 (CVSS score 6.0). Cisco has released free software updates for these vulnerabilities. CISA has reported that this vulnerability has been observed to be actively exploited in the wild. CISA strongly recommends affected Cisco customers apply the patches as quickly as their patch policy allows.

2 Technical Analysis

CVE-2024-20353 (CVSS score 8.6) is a Web Services Denial of Service Vulnerability. An unauthenticated threat actor could remotely reload the Cisco ASA or FTD software. By repeating this exploit, the management and VPN servers would suffer a denial of service (DoS) outage. Threat actors would exploit this vulnerability by sending specially generated HTTP requests to the publicly exposed service. This is one of two zero-day vulnerabilities that have been exploited by threat actors, including ArcaneDoor.

ArcaneDoor is believed to be a state-sponsored cyber espionage group. While researchers are still unsure of the initial intrusion method, backdoors "Line Runner" and "Line Dancer" were observed during campaigns associated with this threat group. Wired reported on this campaign and indicated that this activity appears to align with China's state interests.

CVE-2024-20359 (CVSS score 6.0) is a Persistent Local Code Execution Vulnerability. A preloading of plug-ins and clients could allow unauthenticated local threat actors to execute code with root-level access. The exploit would require already compromised administrator-level access. This vulnerability was caused by improper file validation when read from system flash memory. Threat actors could load a file to disk0 on the file system. Upon the next device reload, the code would be executed. The vulnerability associated with CVE-2024-20358 (CVSS score 6.0) behaves much in the same way but for Linux operating systems.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- For organizations who run Cisco ASA or FTD software, they can check for releases for vulnerabilities on the Cisco Software Checker
- For vulnerable systems, CISA and Cisco recommend applying patch releases to mitigate the risk of exploitation from threat actors

5 References

Cisco Adaptive Security Appliance and Firepower Threat Defense . (2024, April 24). Retrieved April 25, 2024, from https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm

Cisco Adaptive Security Appliance and Firepower Threat Defense . (2024, April 24). Retrieved April 25, 2024, from https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

Cisco Adaptive Security Appliance and Firepower Threat Defense . (2024, April 24). Retrieved April 25, 2024, from https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

Cisco Releases Security Updates Addressing ArcaneDoor . (2024, April 24). Retrieved April 25, 2024, from https://www.cisa.gov/news-events/alerts/2024/04/24/cisco-releases-security-updates-addressing-arcanedoor-vulnerabilities-cisco-firewall-platforms

Cisco Software Checker. Retrieved April 25, 2024, from https://sec.cloudapps.cisco.com/security/center/softwarechecker.x

Greig, J. CISA: Cisco and CrushFTP vulnerabilities are being actively exploited. (2024, April 24). Retrieved April 25, 2024, from https://therecord.media/cisco-asa-crushftp-vulnerabilities-exploited-cisa

NCSC TIP Line Runner. (2024, April 24). Retrieved April 25, 2024, from https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-runner.pdf