

THREAT BULLETINS

Vulnerabilities Observed in Exploit Campaign Affecting Cisco ASA and FTD Software



TLP:WHITE

Apr 25, 2024

On April 24, 2024, Cisco released security [advisories](#) regarding the abuse of vulnerabilities ([CVE-2024-20353](#) and [CVE-2024-20359](#)) identified in campaigns targeting Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software. The malicious activity, dubbed ArcaneDoor, is an operation enacted by state-sponsored threat actors targeting perimeter network devices from multiple vendors. The threat actors intentions behind the operation are likely to pivot into organizations, reroute or modify traffic, and monitor network communications after exploiting affected perimeter network devices.

CVE-2024-20353 is a vulnerability affecting the management and VPN web servers for Cisco Adaptive Security Appliance software and Cisco Firepower Threat Defense software allowing an unauthenticated, remote attacker to negatively impact the uptime of the device by causing unexpected reloads, resulting in a denial of service (DoS) condition.

CVE-2024-20359 is a vulnerability impacting a legacy capability that preloads VPN clients and plug-ins for Cisco Adaptive Security Appliance software and Cisco Firepower Threat Defense software allowing an authenticated, local attacker to execute arbitrary code with escalated privileges. Administrator-level privileges are required to exploit this vulnerability.

According to investigations that took place earlier this year, invoked by a series of events, the activity in question was attributed to a threat actor now identified as UAT4356 and STORM1849 by Cisco Talos and the Microsoft Threat Intelligence Center, respectively. The

threat actor demonstrated a clear focus on espionage and an in-depth knowledge of the devices that they targeted.

Further analysis of the threat group's operations revealed the deployment of two backdoors identified as Line Runner and Line Dancer which were used collectively to conduct targeted actions, including configuration modification, reconnaissance, network traffic capture/exfiltration and potentially lateral movement.

Although the initial attack vectors have yet to be determined, Cisco uncovered a sophisticated attack chain that was used to implant custom malware and execute commands across a small set of users.

Users are strongly advised to follow guidance provided in the full report available [here](#).

Recommendations:

Health-ISAC recommends organizations assess their level of risk to the activity observed as it pertains to the exploitation of the software in question and adhere to the mitigations associated with [CVE-2024-20353](#) and [CVE-2024-20359](#).

Regardless of your network equipment provider, network defenders are encouraged to ensure that the devices are properly patched, logging to a central, secure location, and configured to have strong, multi-factor authentication (MFA).

Reference(s)	
	Cisco , Cisco Talos , Cisco , Cisco

Sources

[ArcaneDoor – New Espionage-Focused Campaign Found Targeting Perimeter Network Devices](#)
[Cisco Event Response: Attacks Against Cisco Firewall Platforms Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability](#)

[Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability](#)

Alert ID b43da293

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

[View Alert](#)

Tags CVE-2024-20359, CVE-2024-20353, Cisco ASA Software, Cisco FTD Software

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.