ADVISORY FOR ICM SECTORS

ArcaneDoor Campaign Targeting Perimeter Network Devices

Original report published on: April 24, 2024[1]

Executive Summary

On April 24, 2024, Cisco Talos released a report shedding light on a campaign by a previously unknown state-sponsored threat actor tracked as "UAT4356". The campaign, dubbed "ArcaneDoor", targeted perimeter network devices from various vendors. Over the past two years, there has been a significant and ongoing rise in the targeting of these devices, and these are used by telecommunications and media organisations.

Two zero-day vulnerabilities were uncovered affecting Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defence (FTD) software that was found exploited. The threat actor exploited CVE-2024-20353 and CVE-2024-20359 to deploy custom malware codenamed "Line Runner" and "Line Dancer".

UAT4356 performed malicious actions such as configuration modification, reconnaissance, network traffic capture/exfiltration, and potentially lateral movement on compromised devices. Cisco released the patches on April 24, 2024, to address these vulnerabilities and mitigate the risks of compromise.

Background

Cisco Talos' investigation found that the UAT4356's infrastructure was established between November and December 2023, with activities first detected in January 2024.

Details of the vulnerabilities are as follows:

a. CVE-2024-20353 (CVSS: 8.6/10.0 - **High**) – Denial of Service (DOS) vulnerability
    i. Successful exploitation of this vulnerability allows an unauthenticated remote attacker to cause the device to reload unexpectedly, resulting in a DOS condition.
    ii. 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.

b. CVE-2024-20359 (CVSS: 6.0/10.0 – **Medium**)– Persistent Local Code Execution vulnerability
    i. Successful exploitation of this vulnerability allows an authenticated local attacker with Administrator-level privileges to execute arbitrary code with root-level privileges.

ii. 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 behaviour. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.

Details of the malware are as follows:

- ***Line Runner*** is a persistent Lua-based webshell targeting the ASA WebVPN device customisation functionality. It exploits Cisco ASA's SSL VPN session to execute arbitrary shellcode, allowing attackers to disable syslog, extract configurations, create packet captures, and run CLI commands without authentication. "Line Dancer" also manipulates crash dumps and authentication systems to hinder forensic analysis and enable unauthorised remote access, forcing a reboot without writing core dumps to avoid detection.

- ***Line Dancer*** is an in-memory implant that enables the uploading and execution of arbitrary shellcode payloads. It exploits a legacy VPN client pre-loading mechanism on Cisco ASA devices, activating at boot from a ZIP file on disk0. It uses a crafted script, csco_config.lua, to install the "Line Dancer" backdoor, ensuring persistence through reboots and upgrades. "Line Runner" sets up scripts and system modifications for remote control while resetting these changes post-activation to cover its tracks. Notably, it modifies the /etc/init.d/unmountfs script to copy the malware ZIP file from a hidden location to disk0 during boot. After installation, it deletes itself from disk to avoid detection.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Initiate scan on your networks using the Indicators of Compromise provided, conduct assessment before blocking them.
- Apply the patches released by Cisco to mitigate CVE-2024-20353 and CVE-2024-20359, if you have the affected devices deployed in your environment.
- Closely monitor inbound and outbound network traffic for suspicious communications or data transmissions.
- Regularly monitor the attack surface and examine any unusual activities that could signal the lateral movement of a threat actor or the presence of malware. Refer to MITRE ATT&CK techniques in this advisory to create detection rules and harden system configuration controls that have no business need.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess potential impacts prior to deploying defensive measures.

Indicators of Compromise[1]

IP Address	Remarks
192.36.57[.]181	Likely Actor-Controlled Infrastructure:
185.167.60[.]85	
185.227.111[.]17	
176.31.18[.]153	
172.105.90[.]154	
185.244.210[.]120	
45.86.163[.]224	
172.105.94[.]93	
213.156.138[.]77	
89.44.198[.]189	
45.77.52[.]253	
103.114.200[.]230	
212.193.2[.]48	
51.15.145[.]37	
89.44.198[.]196	
131.196.252[.]148	
213.156.138[.]78	
121.227.168[.]69	
213.156.138[.]68	
194.4.49[.]6	
185.244.210[.]65	
216.238.75[.]155	
5.183.95[.]95	Multi-Tenant Infrastructure
45.63.119[.]131	
45.76.118[.]87	
45.77.54[.]14	
45.86.163[.]244	
45.128.134[.]189	

89.44.198[.]16	
96.44.159[.]46	
103.20.222[.]218	
103.27.132[.]69	
103.51.140[.]101	
103.119.3[.]230	
103.125.218[.]198	
104.156.232[.]22	
107.148.19[.]88	
107.172.16[.]208	
107.173.140[.]111	
121.37.174[.]139	
139.162.135[.]12	
149.28.166[.]244	
152.70.83[.]47	
154.22.235[.]13	
154.22.235[.]17	
154.39.142[.]47	
172.233.245[.]241	
185.123.101[.]250	
192.210.137[.]35	
194.32.78[.]183	
205.234.232[.]196	
207.148.74[.]250	
216.155.157[.]136	
216.238.66[.]251	
216.238.71[.]49	
216.238.72[.]201	
216.238.74[.]95	
216.238.81[.]149	
216.238.85[.]220	
216.238.86[.]24	

MITRE ATT&CK Tactics and Techniques[1]

Tactic	Technique	ID	Additional Information
Execution	Hooking	T0874	Hooking of the process HostScanReply() function
	Command and Scripting Interpreter	T1059	Execution of CLI commands
Persistence	Boot or Logon Initialization Scripts	T1037	Line Runner persistence mechanism
	Power Settings	T1653	The reboot action via CVE-2024-20353
Defence Evasion	Deobfuscate/Decode Files or Information	T1140	Base64 obfuscation
	Impair Defences: Disable or Modify Tools	T1562.001	Disabling syslog and tampering with AAA
	Process Injection	T1055	Injection of code into AAA and Crash Dump processes
	Modify Authentication Process	T1556	Bypassing of the AAA mechanism
	Indicator Removal: File Deletion	T1070.004	Removal of files after execution
Credential Access	Adversary-in-the-Middle	T1557	HTTP interception for C2 communications
	Network Sniffing	T1040	Network Sniffing

Command and Control	Application Layer Protocol: Web Protocols	TT1071.001	HTTP C2
	Web Service: One-Way Communication	T1102.003	HTTP C2 one-way backdoor
Exfiltration	Exfiltration Over C2 Channel	T1041	Data exfiltration over C2

References

1. ^ “ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices” .