


'ArcaneDoor' Cyberspies Hacked Cisco Firewalls to Access networks

Date: 26th April 2024 | Severity:  High

Summary

Cisco announced the discovery of a new backdoor targeting their Adaptive Security Appliances. The exploitation of two zero-day vulnerabilities in Cisco compromise government targets globally in a hacking campaign it's calling ArcaneDoor.

Attack Vectors

The threat actors deploy two malicious implants:

- Line Dancer is used to execute commands on the compromised device. During our investigation, Talos was able to observe the threat actors using the Line Dancer malware are disabling system logs, providing remote access, Additionally, Line Dancer can manipulate crash dumps and authentication systems, To avoid detection, it modifies the core dump functionality in-memory as an anti-forensics method.
- Line Runner exploits a legacy VPN client pre-loading mechanism on Cisco ASA devices, activating at boot from a ZIP file on disk0. Line Dancer HTTP-based Lua backdoor that remains through reboots and upgrades. Line Dancer employs different security evasion mechanisms. The attackers prepend commands into the / etc/init.d/unmountfs script which is one of the last scripts run before device reboot. These commands copy the malware ZIP file from an administratively inaccessible location to disk0.
- Sophisticated attack chain” involving exploit of the two vulnerabilities — a denial-of-service flaw tracked as CVE-2024-20353 and a persistent local execution flaw tracked as CVE-2024-20359.

Indicator of compromise

INDICATOR TYPE	INDICATORS
IP	<ul style="list-style-type: none"> • 192[.]210[.]137[.]35 • 216[.]238[.]71[.]49 • 139[.]162[.]135[.]12 • 107[.]173[.]140[.]111 • 194[.]32[.]78[.]183 • 216[.]238[.]81[.]149 • 185[.]123[.]101[.]250 • 154[.]39[.]142[.]47 • 107[.]172[.]16[.]208 • 104[.]156[.]232[.]22 • 216[.]155[.]157[.]136 • 207[.]148[.]74[.]250 • 5[.]183[.]95[.]95 • 96[.]44[.]159[.]46 • 89[.]44[.]198[.]16 • 131[.]196[.]252[.]148 • 45[.]77[.]54[.]14 • 194[.]4[.]49[.]6

Recommendation

- There are some known indicators of compromise that customers can look for if they suspect they may have been targeted in this campaign.
- Should look for any flows to/from ASA devices to any of the IP addresses present in the IOC list provided at the bottom of this blog. This is one indication that further investigation is necessary.
- Organizations can issue the command show memory region | include lina to identify another indicator of compromise.
- If organization does find connections to the provided actor IPs and the crash dump functionality has been altered, please open a case with Cisco TAC.

Reference Links

- <https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/>
- <https://www.bleepingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/>
- <https://securityboulevard.com/2024/04/defending-against-arcanedoor-how-eclipsium-protects-network-devices/>
- <https://www.darkreading.com/endpoint-security/cisco-zero-days-arcanedoor-cyberespionage-campaign>