Mphasis
The Next Applied

ArcaneDoor hackers exploit Cisco zero-days to breach government networks

Date: 30th April 2024 | Severity: High

Summary

The hackers, identified as UAT4356 by Cisco Talos and STORM-1849 by Microsoft, began infiltrating vulnerable edge devices in early November 2023 in a cyber-espionage campaign tracked as ArcaneDoor.

Attack Vectors

- Cisco warned today that a state-backed hacking group has been exploiting two zero-day vulnerabilities in Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls.
- The first exploited vulnerability (CVE-2024-20353) stems from an incomplete error checking when parsing an HTTP header. It enables threat actors to trigger a denial of service (DoS) state on the Cisco device by sending a specific HTTP request that forces it to reload unexpectedly.
- The second exploited vulnerability (CVE-2024-20359) is a legacy capability that enables the preloading of VPN clients and plug-ins by an authenticated, local attacker. Notably, the attacker needs to have administrator-level privileges to exploit it and execute arbitrary code on the device.
- Line Dancer - an in-memory backdoor used to upload and execute arbitrary shellcode payloads for disabling system logs, providing remote access, and exfiltrating internet traffic packet captures. To avoid detection, this backdoor evades the generation of forensics data through a crash dump when the system reboots.
- Line Runner - an HTTP-based Lua backdoor used to establish persistence and to retrieve information staged by Line Dancer. These backdoor employs different security evasion mechanisms.

Indicator of compromise

INDICATOR TYPE	INDICATORS	
IPs	• 185.244.210.65 • 139.162.135.12 • 216.238.75.155 • 103.119.3.230 • 154.22.235.17 • 107.148.19.88 • 192.210.137.35 • 103.51.140.101 • 216.238.72.201 • 216.238.86.24 • 89.44.198.16 • 103.125.218.198 • 205.234.232.196 • 185.123.101.250 • 96.44.159.46 • 149.28.166.244 • 107.172.16.208 • 45.76.118.87 • 216.238.71.49 • 207.148.74.250 • 216.238.66.251 • 45.63.119.131 • 154.39.142.47 • 154.22.235.13 • 5.183.95.95 • 216.238.85.220 • 121.37.174.139	• 104.156.232.22 • 216.238.74.95 • 152.70.83.47 • 216.155.157.136 • 194.32.78.183 • 103.27.132.69 • 103.20.222.218 • 216.238.81.149 • 45.77.54.14 • 45.128.134.189 • 107.173.140.111 • 45.86.163.244 • 172.233.245.241 • 212.193.2.48 • 213.156.138.78 • 89.44.198.196 • 89.44.198.189 • 51.15.145.37 • 121.227.168.69 • 213.156.138.68 • 45.86.163.224 • 103.114.200.230 • 213.156.138.77 • 185.244.210.120 • 192.36.57.181 • 185.227.111.17 • 194.4.49.6

Recommendation

- All customers to upgrade their devices to fixed software to block any incoming attacks.
- Security administrators should block the IoCs on all applicable security solutions post-validation.
- Users are recommended to update and fix to the latest versions of Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Firewalls as soon as possible post testing.
- Organizations are recommended to have a behavioral detection solution in place to successfully detect the presence of malware payloads.
- Users are recommended to use a unique and strong password at every site with the help of a password manager and use multi factor authentication whenever possible.
- Organizations are recommended to servers have a behavioral detection solution in place to successful detect the presence of malware payloads.
- Security administrators should apply the principle of least privilege to all systems and services.
- Keep AV signatures, operating systems, and third-party applications up to date on all systems, mobile devices, and servers.

Reference Links

- https://www.bleepingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/?&web_view=true
- https://varutra.com/ctp/threatpost/postDetails/Hackers-Exploit-Cisco-Zero-Days-to-Breach-Government-Networks/Rk5sNysvV1kvTWYrWmRRSHZwckxaUT09