Network Device Threats Timeline_

SUMMARY

2005
First Cisco Rootkit

2008
Operation Cisco Raider

2015
SYNful Knock
Cisco ROMMON Attack
Juniper Backdoors

2016
Shadow Brokers

2017
Vault 7 Leak

2018
VPNFilter Campaign
Cisco Backdoors

2019
FortiOS Vulnerability
Echobot

2020
Citrix Vulnerability
Pulse VPN Campaign
Fox Kitten Campaign
Sophos Zero-Day
F5 1st 10.0 CVSS
Netwalker Attacks
Chinese Attacks

2021
Cring Ransomware
Pulse Secure Vulnerabilities
F5 Vulnerabilities
SonicWall Vulnerabilities
Fortinet Attack

2022
Cyclops Blink
F5 BIG-IP Vulnerability
Citrix APT Campaign
FortiGate Zero-Day

2023
Fortinet Zero-Day
Jaguar Tooth Malware
Zyxel-based Botnet
Volt Typhoon
Fortinet Exploit
CISA Directive
Citrix Zero-day
Akira and Lockbit
BlackTech
Cisco Zero-Days
Citrix Zero-Day

2024
Ivanti Zero-Days

2005

Independent security researcher Mike Lynn demonstrates the first-ever Cisco IOS rootkit at the Black Hat conference.[1][2]

2008

The FBI concludes Operation Cisco Raider, a two-year initiative to disrupt a Cisco distribution network that had sold counterfeit Cisco gear to the U.S. military and other organizations.[3]

2015

SYNful Knock malware targets Cisco IOS devices, installing an implant that provides persistent access that is difficult to detect.[4] NATION-STATE

Cisco warns customers about attacks that swap ROMMON remote management firmware with maliciously altered images.[5]

Juniper discloses a supply chain attack where two backdoors were implanted in its NetScreen VPN products. Researchers attribute the backdoors to the NSA.[6] NATION-STATE

2016

The Shadow Brokers release hacking tools from the Equation Group, thought to be the NSA. The tools contain zero-day exploits of Cisco, Fortinet, and Juniper firewalls.[7] NATION-STATE

2017

Wikileaks' Vault 7 leak exposes tools used by the CIA and leads to the discovery of CVE-2017-3881 affecting 300+ Cisco routers and switches.[8] NATION-STATE

2018

The VPNFilter campaign infects 500K+ devices worldwide from Linksys, MikroTik, Netgear, and TP-Link. The malware has data collection and destructive capabilities, and is attributed to the Russian Sandworm threat group.[9] NATION-STATE

Five backdoors discovered in Cisco products raise worries about a supply chain attack. One of the backdoors is an undocumented user account with privilege level 15 that has a default username and password in Cisco IOS.[10]

2019

CVE-2018-13379 is discovered in the FortiOS SSL VPN web portal. This vulnerability is subsequently listed among CISA's Top 12 Routinely Exploited Vulnerabilities in 2020, 2021, and 2022, underscoring the difficulty in patching network appliances.[11]

Echobot, a variant of the Mirai botnet malware, targets SCADA systems and enterprise networking gear, including Barracuda and Citrix appliances.[12]

2020

Security researchers detail a campaign targeting Citrix ADCs as entry points to disable Windows Defender and install Ragnarok ransomware on Windows machines in the network.[13] RANSOMWARE

Criminals launch a wide-scale campaign targeting Pulse Secure VPN appliances to steal Active Directory credentials, disable endpoint security, and install REvil ransomware.[14] RANSOMWARE

Security researchers detail the techniques of the Iranian-backed Fox Kitten campaign, whose primary method of initial access is VPN devices from Citrix, Fortinet, Palo Alto Networks, and Pulse Secure.[15] NATION-STATE

COVID-19 restrictions in March put a focus on the security and availability of VPN infrastructure as employees connect remotely.[16]

Sophos alerts customers to a zero-day exploit against its XG firewalls that deploys the Asnarök data-stealing trojan and then attempts to install Ragnarok ransomware. The attacks are foiled by a hotfix from the vendor.[17] RANSOMWARE

F5 discloses its first-ever vulnerability with a CVSS of 10.0. Public exploits are available within a week and the vulnerability is widely exploited.[18]

The FBI releases IOCs for widespread Netwalker ransomware attacks that target vulnerable Pulse Secure VPN devices for initial access.[19] RANSOMWARE

CISA issues a cybersecurity advisory to help U.S. government agencies defend against Chinese state-sponsored attack activity, which includes exploiting recent vulnerabilities in F5 BIG-IP, Citrix VPN, and Pulse Secure VPN appliances.[20] NATION-STATE

2021

Kaspersky details techniques used by attackers to install Cring ransomware in enterprise victims. Initial access focused on vulnerable FortiGate VPN appliances.[21] RANSOMWARE

Multiple campaigns target vulnerabilities in Pulse Secure VPN appliances, including a zero-day (CVE-2021-22893). Mandiant tracks 12 separate malware families targeting Pulse Secure devices and also says Chinese state-sponsored groups exploit these vulnerabilities for espionage.[22][23] NATION-STATE

F5 publishes a security advisory containing 21 CVEs, including four critical vulnerabilities. CVE-2021-22986 is later observed as an initial access vector for Lockbit 3.0.[24] RANSOMWARE

Dozens of critical vulnerabilities involving SQL injection, buffer overflow, out-of-bound read, etc. are discovered in SonicWall devices. Mandiant notes the ransomware group UNC2447 uses some of these exploits for initial access and persistence.[25][26] RANSOMWARE

Hackers publish a list of credentials stolen from 87K Fortinet devices on a ransomware forum. The credentials were harvested using a vulnerability from 2018.[27] RANSOMWARE

2022

Cyclops Blink malware targets Watchguard firewalls and ASUS routers, and is attributed to the Russian Sandworm threat group. In a court-authorized operation, the FBI disabled the botnet by removing the malware and closing external management ports on infected devices used for C2.[28] NATION-STATE

CVE-2022-1388 affects F5 BIG-IP devices and is listed among CISA Top 12 Routinely Exploited Vulnerabilities for 2022.[29]

The NSA releases threat hunting guidance for Citrix ADC devices targeted by APT5 as part of its espionage activities. Recommendations include checking hashes of important binaries, monitoring logs, and running YARA rules to look for specific malware used.[30] NATION-STATE

A critical zero-day vulnerability (CVE-2022-42475) is discovered in FortiGate firewalls during an incident investigation by the vendor.[31]

2023

March

Another Fortinet zero-day is discovered (CVE-2022-41328) being exploited by Chinese hackers (UNC3886), who use the appliances as a pivot to ESXi infrastructure and then to VM guests.[32] NATION-STATE

April

The U.K. National Cyber Security Centre releases a report warning of Jaguar Tooth malware targeting Cisco IOS. NATION-STATE

May

Security researchers observe widespread exploitation of CVE-2023-28771 in Zyxel devices to build a Mirai-based botnet.[33] NATION-STATE

22 Danish energy firms are compromised in a campaign that exploited CVE-2023-28771 as well as two new zero-day vulnerabilities in Zyxel devices (CVE-2023-33009 and CVE-2023-33010). The attacks were attributed to the Russian Sandworm group.[34] NATION-STATE

Microsoft publishes details of its investigation into the Chinese Volt Typhoon group targeting U.S. critical infrastructure. The attackers use an unknown Fortinet exploit and use routers from ASUS, Cisco, D-Link, NETGEAR, and Zyxel as proxies for C2 traffic.[35] NATION-STATE

In response to an ongoing campaign utilizing a zero-day vulnerability (CVE-2023-2868) against Barracuda appliances, the vendor recommends that customers return their appliances for new ones.[36]

June

CISA directs federal agencies to either implement zero-trust for network management interfaces or remove them from the internet.[37]

July

CVE-2023-3519 is discovered as a zero-day in Citrix Netscalers and mass exploitation commences within weeks, compromising 30K+ devices. The campaign is attributed to the ransomware actor FIN8.[38] RANSOMWARE

August

Rapid7 responds to a number of incidents involving Cisco ASA SSL VPNs, some involving ransomware gangs Akira and Lockbit. Less than two weeks later, Cisco discloses CVE-2023-20269 which is related. RANSOMWARE

September

The NSA and the Japanese government issue a warning about the Chinese group BlackTech targeting "various brands and versions" of routers to install implants for espionage.[39] NATION-STATE

October

Cisco discovers a campaign exploiting two zero-day vulnerabilities (CVE-2023-20198 and CVE-2023-20273) to create admin accounts and install implants on Cisco IOS XE devices. Before a patch is available, at least 10K devices are infected.[40]

A zero-day vulnerability (CVE-2023-4966) dubbed Citrix Bleed is discovered. Mandiant reports threat activity since August, allowing attackers to hijack authenticated sessions. Lockbit and ALPHV/BlackCat use Citrix Bleed to compromise numerous organizations, including Boeing, ICBC, Toyota Financial Services, DP World, and Fidelity National Financial.[41] RANSOMWARE

2024

January

Ivanti discloses two zero-day vulnerabilities in its Connect Secure (formerly Pulse Secure) VPN product observed to be exploited by a Chinese nation-state attacker since December. Mass exploitation begins soon after proof-of-concept code is published, while no patch is available for weeks.[42] CISA issues an emergency directive ordering federal civilian agencies to mitigate the vulnerabilities with configuration changes and an integrity checker tool.[43] NATION-STATE

1. *The Holy Grail: Cisco IOS Shellcode And Exploitation Techniques*, Michael Lynn, July 2008
2. *An Insider's View of 'Cisco-gate'*, WIRED, August 2005
3. *FBI probe discovers counterfeit kit in US military networks*, The Register, May 2008
4. SYNful Knock
5. *Attackers are hijacking critical networking gear from Cisco, company warns*, Ars Technica, August 2015
6. *Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA*, WIRED, December 2015
7. *Equation Group exploit hits newer Cisco ASA*, Juniper Netscreen, The Register, August 2016
8. *The Wikileaks Vault 7 Leak – What We Know So Far*, Cisco Blogs, March 2017
9. VPNFilter
10. *Backdoors Keep Appearing In Cisco's Routers*, Tom's Hardware, July 2018
11. *2022 Top Routinely Exploited Vulnerabilities*, CISA, August 2023
12. *Echobot Malware Now up to 71 Exploits, Targeting SCADA*, F5 Labs, December 2019
13. *Ragnarok Ransomware Targets Citrix ADC, Disables Windows Defender*, Bleeping Computer, January 2020
14. *VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers*, ZDNet, January 2020
15. *Fox Kitten Campaign Widespread Iranian Espionage-Offensive Campaign*, Clearsky Cybersecurity, February 2020
16. *Cybersecurity Advisory: Enterprise VPN Security*, CISA, April 2020
17. *Hackers tried to use Sophos Firewall zero-day to deploy Ransomware*, Bleeping Computer, May 2020
18. *Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902*, CISA, July 2020
19. *FBI Flash: Indicators Associated with Netwalker Ransomware*, FBI, July 2020
20. *Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity*, CISA, December 2020
21. *Vulnerability in FortiGate VPN servers is exploited in Cring ransomware attacks*, Kaspersky, April 2021
22. *Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day*, Mandiant, April 2021
23. *Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices*, Mandiant, May 2021
24. *LockBit: Access, Encryption, Exfiltration, & Mitigation*, November 2023
25. *UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat*, Mandiant, April 2021
26. *SonicWall Zero-Day Exploited by Ransomware Group Before It Was Patched*, SecurityWeek, April 2021
27. *Fortinet warns customers after hackers leak passwords for 87,000 VPNs*, The Record, September 2021
28. *Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)*, U.S. Department of Justice, April 2022.
29. *2022 Top Routinely Exploited Vulnerabilities*, CISA, August 2023
30. *APT5: Citrix ADC Threat Hunting Guidance*, NSA, December 2022
31. *We're Out of Titles for VPN Vulns—It's Not Funny Anymore*, WatchTowr, January 2023
32. *Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation*, Mandiant, March 2023
33. *Hackers exploit critical Zyxel firewall flaw in ongoing attacks*, BleepingComputer, May 2023
34. *Russian Hackers Linked to 'Largest Ever Cyber Attack' on Danish Critical Infrastructure*, The Hacker News, November 2023
35. *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques*, Microsoft, May 2023
36. *Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China*, Mandiant, June 2023
37. *BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces*, CISA, June 2023
38. *Attacks on Citrix NetScaler systems linked to ransomware actor*, BleepingComputer, July 2023
39. *People's Republic of China-Linked Cyber Actors Hide in Router Firmware*, NSA, September 2023
40. *"Cisco buried the lede." >10,000 network devices backdoored through unpatched 0-day*, ArsTechnica, October 2023
41. *Remediation for Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966)*, Mandiant, October 2023
42. *Ivanti Connect Secure VPN Exploitation Goes Global*, Volexity, January 2024
43. *ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*, CISA, January 2024