Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

9 February 2024

Vulnerabilities

New Fortinet RCE flaw in SSL VPN likely exploited in attacks

Bleeping Computer - February 8 2024

Fortinet is warning that a new critical remote code execution vulnerability in FortiOS SSL VPN is potentially being exploited in attacks. The flaw (tracked as CVE-2024-21762 / FG-IR-24-015) received a 9.6 severity rating and is an out-of-bounds write vulnerability in FortiOS that allows unauthenticated attackers to gain remote code execution (RCE) via maliciously crafted requests.

February 2024 Patch Tuesday forecast: Zero days are back and a new server too

Help Net Security - February 9 2024

January 2024 Patch Tuesday is behind us. A relatively light release from Microsoft with 39 CVEs addressed in Windows 10, 35 in Windows 11, and surprisingly no zero-day vulnerabilities from Microsoft to start the new year.

CISA Releases Two Industrial Control Systems Advisories

CISA Current Activity - February 8 2024

CISA released two Industrial Control Systems (ICS) advisories on February 8, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-039-01 Qolsys IQ Panel 4, IQ4 HUB ICSA-23-082-06 ProPump and Controls Osprey Pump Controller (Update A) CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

MalDocs in Word and Excel: A Persistent Cybersecurity Challenge

Check Point - February 8 2024

Despite being several years old, CVEs from 2017 and 2018 in Microsoft Word and Excel remain active threats in the cybersecurity landscape. Examples include CVE-2017-11882, CVE-2017-0199, and CVE-2018-0802. These vulnerabilities are exploited by well-known malware such as GuLoader, Agent Tesla, Formbook, and others.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Ransomware

Patterns and Targets for Ransomware Exploitation of Vulnerabilities: 2017–2023

Recorded Future - Blog - February 8 2024

Recent Insikt research analyzes ransomware and vulnerability trends spanning the past six years and offers insights into future expectations. Ransomware groups exploit vulnerabilities in two distinct categories: those targeted by only a few groups and those widely exploited by several. Each category necessitates different defense strategies.

Malware and threat actors

'Ov3r_Stealer' Malware Spreads Through Facebook to Steal Crates of Info

Dark Reading - February 8 2024

A novel stealer malware called "Ov3r_Stealer" is making the rounds on Facebook, spreading through job ads and accounts on the social media platform, and using various execution methods to steal reams of data from unwitting victims.

Akira, LockBit actively searching for vulnerable Cisco ASA devices

Help Net Security - February 8 2024

Akira and Lockbit ransomware groups are trying to breach Cisco ASA SSL VPN devices by exploiting several older vulnerabilities, security researcher Kevin Beaumont is warning.

China-linked APT Volt Typhoon remained undetected for years in US infrastructure

Security Affairs - February 8 2024

China-linked APT Volt Typhoon infiltrated a critical infrastructure network in the US and remained undetected for at least five years. US CISA, the NSA, the FBI, along with partner Five Eyes agencies, published a joint advisory to warn that China-linked APT Volt Typhoon infiltrated a critical infrastructure network in the US and remained undetected for at least five years.