Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

15 February 2024

Vulnerabilities

Zoom patches critical privilege elevation flaw in Windows apps

Bleeping Computer - February 14 2024

The Zoom desktop and VDI clients and the Meeting SDK for Windows are vulnerable to an improper input validation flaw that could allow an unauthenticated attacker to conduct privilege escalation on the target system over the network.

Zero-Day in QNAP QTS Affects NAS Devices Globally

HackRead - February 14 2024

QNAP has released fixes for the zero-day vulnerability, so it's important to install them immediately.

Microsoft: New critical Exchange bug exploited as zero-day

Bleeping Computer - February 14 2024

Microsoft warned today in an updated security advisory that a critical vulnerability in Exchange Server was exploited as a zero-day before being fixed during this month's Patch Tuesday. Discovered internally and tracked as CVE-2024-21410, this security flaw can let remote unauthenticated threat actors escalate privileges in NTLM relay attacks targeting vulnerable Microsoft Exchange Server versions.

Microsoft patches 2 exploited zero-days, 5 critical vulnerabilities

SC Magazine US - February 14 2024

Two zero-day vulnerabilities actively exploited by ransomware threat groups were among 73 bugs Microsoft addressed in this month’s Patch Tuesday release. The zero-days included a bug that allows hackers to bypass a security feature designed to protect against malicious internet shortcut files, and another that allows attackers to bypass SmartScreen security checks. February’s batch of 73 patches — up from the 48 released last month — included fixes for five bugs rated "critical".

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Malware and threat actors

Microsoft, OpenAI reveal ChatGPT use by state-sponsored hackers

SC Magazine US - February 14 2024

Microsoft and OpenAI revealed Wednesday that Fancy Bear, Kimsuky and three other state-sponsored threat actors have used ChatGPT as part of their cybercrime operations. Large language models (LLMs), including ChatGPT, were leveraged by Russian, North Korean, Iranian and Chinese nation-state hacking groups for scripting and phishing help, vulnerability research, target reconnaissance, detection evasion and more, as outlined in a blog post by Microsoft Threat Intelligence.

China's Volt Typhoon spies broke into emergency network of 'large' US city

The Register - Security - February 14 2024

The Chinese government's Volt Typhoon spy team has apparently already compromised a large US city's emergency services network and has been spotted snooping around America's telecommunications' providers as well.

Water Hydra’s Zero-Day Attack Chain Targets Financial Traders

Infosecurity Today - February 14 2024

CVE-2024-21412 was used to evade Microsoft Defender SmartScreen and implant victims with DarkMe

BumbleBee Malware Buzzes Back on the Scene After 4-Month Hiatus

Dark Reading - February 14 2024

The sophisticated Bumblebee loader is back in the threat landscape hive after a four-month hiatus, with a new email campaign targeting thousands of organizations in the US. Bumblebee, an initial access loader used by multiple cybercriminal groups to drop various payloads like infostealers, banking Trojans, and post-compromise tools, first appeared on the scene in March 2022.