Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

26 March 2024

Vulnerabilities

CISA Adds Three Known Exploited Vulnerabilities to Catalog
CISA Current Activity - March 25 2024

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-48788 Fortinet FortiClient EMS SQL Injection Vulnerability CVE-2021-44529 Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability CVE-2019-7256 Nice Linear eMerge E3-Series OS Command Injection Vulnerability These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

CISA urges software devs to weed out SQL injection vulnerabilities
Bleeping Computer - March 25 2024

CISA and the FBI urged executives of technology manufacturing companies to prompt formal reviews of their organizations' software and implement mitigations to eliminate SQL injection (SQLi) security vulnerabilities before shipping. In SQL injection attacks, threat actors "inject" maliciously crafted SQL queries into input fields or parameters used in database queries, exploiting vulnerabilities in the application's security to execute unintended SQL commands, such as exfiltrating, manipulating, or deleting sensitive data stored in the database.

Malware and threat actors

StrelaStealer malware hits more than 100 EU and US organizations
SC Media - March 25 2024

Security pros say StrelaStealer uses control flow obfuscation — a technique that lets the threat actor better evade detection and reverse engineering.

Newly detailed Tycoon 2FA phishing kit bypasses multi-factor authentication
SiliconANGLE - March 25 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Cybersecurity researchers at Sekoia ApS' Threat Detection & Research team are warning of a new phishing kit linked to the adversary-in-the-middle technique that is being utilized by multiple threat actors to conduct effective attacks. Called "Tycoon 2FA," the phishing kit has been active since at least August 2023 and is claimed to now be one the most prevalent AiTM phishing kits, with over 1,100 domain names detected between October 2023 and February 2024.

US sanctions APT31 hackers behind critical infrastructure attacks

Bleeping Computer - March 25 2024

The U.S. Treasury Department has sanctioned a Wuhan-based company used by the Chinese Ministry of State Security (MSS) as cover in attacks against U.S. critical infrastructure organizations. The Office of Foreign Assets Control (OFAC) has also designated two Chinese nationals (Zhao Guangzong and Ni Gaobin) linked to the APT31 Chinese state-backed hacking group and who worked as contractors for the Wuhan Xiaoruizhi Science and Technology Company, Limited (Wuhan XRZ) MSS front company for their involvement in the same attacks and "endangering U.S. national security."

Key Lesson from Microsoft's Password Spray Hack: Secure Every Account

The Hacker News - March 25 2024

In January 2024, Microsoft discovered they'd been the victim of a hack orchestrated by Russian-state hackers Midnight Blizzard (sometimes known as Nobelium). The concerning detail about this case is how easy it was to breach the software giant.