Scottish Cyber Coordination Centre

Daily threat bulletin

25 September 2024

Vulnerabilities

CISA Flags Critical Ivanti vTM Vulnerability Amid Active Exploitation Concerns

The Hacker News - 25 September 2024 12:31

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a critical security flaw impacting Ivanti Virtual Traffic Manager (vTM) to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.The vulnerability in question is CVE-2024-7593 (CVSS score: 9.8).

Critical Automated Tank Gauge Bugs Threaten Critical Infrastructure

darkreading - 24 September 2024 20:12

The security vulnerabilities could lead to everything from gas spills to operations data disclosure, affecting gas stations, airports, military bases, and other hypersensitive locations.

[R1] Nessus Network Monitor 6.5.0 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 24 September 2024 16:43

[R1] Nessus Network Monitor 6.5.0 Fixes Multiple Vulnerabilities.

Threat actors and malware

Infostealer malware bypasses Chrome's new cookie-theft defenses

BleepingComputer - 24 September 2024 14:31

Infostealer malware developers released updates claiming to bypass Google Chrome's recently introduced feature App-Bound Encryption to protect sensitive data such as cookies. [...]

RomCom Malware Resurfaces With SnipBot Variant

darkreading - 24 September 2024 10:15

The latest version of the evolving threat is a multistage attack demonstrating a move away from ransomware to purely espionage activities, typically targeting Ukraine and its supporters.

AI-Generated Malware Found in the Wild

SecurityWeek - 24 September 2024 17:15

HP has intercepted an email campaign comprising a standard malware payload delivered by an AI-generated dropper.

Scottish Cyber Coordination Centre

Threat Actors Shift to JavaScript-Based Phishing Attacks

Infosecurity Magazine - 24 September 2024 17:30

Cybercriminals are increasingly prioritizing script-based phishing techniques over one based on traditional malicious documents

New Octo2 Malware Variant Threatens Mobile Banking Security

Infosecurity Magazine - 24 September 2024 16:30

Cybercriminals have been observed disguising Octo2 as legitimate apps like Google Chrome and NordVPN.

SANS Institute: Top 5 dangerous cyberattack techniques in 2024

Security Intelligence - 24 September 2024 14:00

The SANS Institute — a leading authority in cybersecurity research, education and certification — released its annual Top Attacks and Threats Report. This report provides insights into the evolving threat landscape, identifying the most prevalent and dangerous cyberattack techniques that organizations need to prepare for.