Scottish Cyber Coordination Centre

Daily Threat Bulletin

14 August 2025

Vulnerabilities

Critical FortiSIEM flaw under active exploitation, Fortinet warns

Security Affairs - 13 August 2025 18:40

Fortinet warns customers of a critical vulnerability, tracked as CVE-2025-25256 (CVSS score of 9.8), affecting FortiSIEM for which an exploit exists in the wild.

Spike in Fortinet VPN brute-force attacks raises zero-day concerns

BleepingComputer - 13 August 2025 13:42

A massive spike in brute-force attacks targeted Fortinet SSL VPNs earlier this month, followed by a switch to FortiManager, marked a deliberate shift in targeting that has historically preceded new vulnerability disclosures.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-8875 N-able N-central Insecure Deserialization Vulnerability

CVE-2025-8876 N-able N-central Command Injection Vulnerability

Chipmaker Patch Tuesday: Many Vulnerabilities Addressed by Intel, AMD, Nvidia

SecurityWeek - 13 August 2025 13:29

Intel, AMD and Nvidia have published security advisories describing vulnerabilities found recently in their products.

Zoom and Xerox Release Critical Security Updates Fixing Privilege Escalation and RCE Flaws

The Hacker News - 13 August 2025 19:49

Zoom and Xerox have addressed critical security flaws in Zoom Clients for Windows and FreeFlow Core that could allow privilege escalation and remote code execution.

Scottish
Cyber
Coordination
Centre

Threat actors and malware

New downgrade attack can bypass FIDO auth in Microsoft Entra ID

BleepingComputer - 13 August 2025 16:14

Security researchers have created a new FIDO downgrade attack against Microsoft Entra ID that tricks users into authenticating with weaker login methods, making them susceptible to phishing and session hijacking.

New PS1Bot Malware Campaign Uses Malvertising to Deploy Multi-Stage In-Memory Attacks

The Hacker News - 13 August 2025 22:16

Cybersecurity researchers have discovered a new malvertising campaign that’s designed to infect victims with a multi-stage malware framework called PS1Bot. PS1Bot features a modular design, with several modules delivered used to perform a variety of malicious activities on infected systems, including information theft, keylogging, reconnaissance, and the establishment of persistent system.

US Authorities Seize $1m from BlackSuit Ransomware Group

Infosecurity Magazine - 13 August 2025 10:30

The US Department of Justice has announced the seizure of domains, servers and $1m in proceeds from the BlackSuit ransomware group