Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 October 2025

Vulnerabilities

Windows Server Update Services (WSUS) vulnerability abused to harvest sensitive data

Threat Research – Sophos News - 29 October 2025 20:46

Exploitation of CVE-2025-59287 began after public disclosure and the release of proof-of-concept code.

Active Exploits Hit Dassault and XWiki — CISA Confirms Critical Flaws Under Attack

The Hacker News - 29 October 2025 14:14

Threat actors are actively exploiting multiple security flaws impacting Dassault Systèmes DELMIA Apriso and XWiki, according to alerts issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and VulnCheck.

Threat actors and malware

PhantomRaven attack floods npm with credential-stealing packages

BleepingComputer - 29 October 2025 13:26

An active campaign named ‘PhantomRaven’ is targeting developers with dozens of malicious npm packages that steal authentication tokens, CI/CD secrets, and GitHub credentials.

New Attack Targets DDR5 Memory to Steal Keys From Intel and AMD TEEs

SecurityWeek - 29 October 2025 08:45

Intel and AMD have published advisories after academics disclosed details of the new TEE.fail attack method.

Russian hackers, likely linked to Sandworm, exploit legitimate tools against Ukrainian targets

Security Affairs - 29 October 2025 15:56

Russian threat actors, likely linked to the APT Sandworm, targeted Ukrainian organizations to steal sensitive data and maintain long-term network access.

Experts Reports Sharp Increase in Automated Botnet Attacks Targeting PHP Servers and IoT Devices

The Hacker News - 29 October 2025 22:08

Cybersecurity researchers are calling attention to a spike in automated attacks targeting PHP servers, IoT devices, and cloud gateways by various botnets such as Mirai, Gafgyt, and Mozi.