Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 November 2025

Vulnerabilities

Microsoft: Patch for WSUS flaw disabled Windows Server hotpatching

BleepingComputer - 03 November 2025 11:22

An out-of-band (OOB) security update that patches an actively exploited Windows Server Update Service (WSUS) vulnerability has broken hotpatching on some Windows Server 2025 devices. [...]

Chrome 142 Released: Two high-severity V8 flaws fixed, $100K in rewards paid

Security Affairs - 03 November 2025 15:55

Google released Chrome 142, fixing 20 flaws, including two high-severity V8 bugs, and awarded $100,000 in bug bounties. Google addressed 20 flaws in Chrome version 142, including high-severity bugs that impact the V8 engine. The IT giant awarded $100,000 in bounties for two issues in the V8 JavaScript engine.

New GDI Flaws Could Enable Remote Code Execution in Windows

Infosecurity Magazine - 03 November 2025 17:00

Flaws in Windows Graphics Device Interface (GDI) have been identified that allow remote code execution and information disclosure

Threat actors and malware

Microsoft: SesameOp malware abuses OpenAI Assistants API in attacks

BleepingComputer - 03 November 2025 14:35

Microsoft security researchers have discovered a new backdoor malware that uses the OpenAI Assistants API as a covert command-and-control channel. [...]

US cybersecurity experts indicted for BlackCat ransomware attacks

BleepingComputer - 03 November 2025 13:15

Three former employees of cybersecurity incident response companies DigitalMint and Sygnia have been indicted for allegedly hacking the networks of five U.S. companies in BlackCat (ALPHV) ransomware attacks between May 2023 and November 2023. [...]

Hackers use RMM tools to breach freighters and steal cargo shipments

BleepingComputer - 03 November 2025 12:46

Scottish Cyber Coordination Centre

Threat actors are targeting freight brokers and trucking carriers with malicious links and emails to deploy remote monitoring and management tools (RMMs) that enable them to hijack cargo and steal physical goods. [...]

New HttpTroy Backdoor Poses as VPN Invoice in Targeted Cyberattack on South Korea

The Hacker News - 03 November 2025 17:12

The North Korea-linked threat actor known as Kimsuky has distributed a previously undocumented backdoor codenamed HttpTroy as part of a likely spear-phishing attack targeting a single victim in South Korea.

'TruffleNet' Attack Wields Stolen Credentials Against AWS

darkreading - 03 November 2025 11:59

Reconnaissance and BEC are among the malicious activities attackers commit after compromising cloud accounts, using a framework based on the TruffleHog tool.