Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

19 September 2025

Vulnerabilities

CVE-2025-10585 is the sixth actively exploited Chrome zero-day patched by Google in 2025

Security Affairs - 18 September 2025 09:57

Google released security updates to address four vulnerabilities in the Chrome web browser, including CVE-2025-10585, which has reportedly been exploited in the wild.

CISA Warns of Two Malware Strains Exploiting Ivanti EPMM CVE-2025-4427 and CVE-2025-4428

The Hacker News - 19 September 2025 10:40

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday released details of two sets of malware that were discovered in an unnamed organization’s network following the exploitation of security flaws in Ivanti Endpoint Manager Mobile (EPMM).

OpenAI fixes zero-click ShadowLeak vulnerability affecting ChatGPT Deep Research agent

The Record from Recorded Future News - 18 September 2025 21:42

OpenAI fixed a vulnerability that could have allowed attackers to steal sensitive information through ChatGPT’s Deep Research agent.

Threat actors and malware

SonicWall Prompts Password Resets After Hackers Obtain Firewall Configurations

SecurityWeek - 18 September 2025 10:41

The company sent a new preferences file to less than 5% of customers, urging them to import it into firewalls and reset their passwords.

News alert: Palo Alto flags threats that evade Secure Web Gateways — echoing SquareX research

Security Boulevard - 18 September 2025 21:52

Despite responsible disclosures to all major SASE/SSE providers at DEF CON 32 last year, no vendor has made an official statement to warn its customers about the vulnerability in the past 13 months – until two weeks ago.

SilentSync RAT Delivered via Two Malicious PyPI Packages Targeting Python Developers

The Hacker News - 18 September 2025 18:08

Cybersecurity researchers have discovered two new malicious packages in the Python Package Index (PyPI) repository that are designed to deliver a remote access trojan called SilentSync on Windows systems.

SystemBC malware turns infected VPS systems into proxy highway

BleepingComputer - 18 September 2025 11:35

The operators of the SystemBC proxy botnet are hunting for vulnerable commercial virtual private servers (VPS) and maintain an average of 1,500 bots every day that provide a highway for malicious traffic.

CountLoader Broadens Russian Ransomware Operations With Multi-Version Malware Loader

The Hacker News - 18 September 2025 19:26

Cybersecurity researchers have discovered a new malware loader codenamed CountLoader that has been put to use by Russian ransomware gangs to deliver post-exploitation tools like Cobalt Strike and AdaptixC2, and a remote access trojan known as PureHVNC RAT.

UK incidents

UK arrests 'Scattered Spider' teens linked to Transport for London hack

BleepingComputer - 18 September 2025 11:37

Two teenagers, believed to be linked to the August 2024 cyberattack on Transport for London, have been arrested in the United Kingdom.