Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

28 November 2025

Vulnerabilities

QNAP warns of critical ASP.NET flaw in its Windows backup software

BleepingComputer - 27 October 2025 13:55

QNAP warned customers to patch a critical ASP.NET Core vulnerability that also impacts the company's NetBak PC Agent, a Windows utility for backing& up data to a QNAP network-attached storage (NAS) device. [...]

Wordfence blocks 8.7M attacks exploiting old GutenKit and Hunk Companion flaws

Security Affairs - 27 October 2025 09:40

Hackers exploited old RCE flaws in WordPress GutenKit and Hunk Companion plugins. Wordfence firm blocked 8.7M attacks in two days. In September and October 2024, submissions revealed Arbitrary Plugin Installation vulnerabilities in GutenKit and Hunk Companion WordPress plugins, with 40,000 and 8,000+ installs, respectively.

Researchers exploit OpenAI's Atlas by disguising prompts as URLs

The Register - 27 October 2025 14:54

NeuralTrust shows how agentic browser can interpret bogus links as trusted user commands Researchers have found more attack vectors for OpenAI's new Atlas web browser – this time by disguising a potentially malicious prompt as an apparently harmless URL....

Year-Old WordPress Plugin Flaws Exploited to Hack Websites

SecurityWeek - 27 October 2025 11:46

Roughly 9 million exploit attempts were observed this month as mass exploitation of the critical vulnerabilities recommenced.

Threat actors and malware

Ransomware profits drop as victims stop paying hackers

BleepingComputer - 27 October 2025 16:22

The number of victims paying ransomware threat actors has reached a new low, with just 23% of the breached companies giving in to attackers' demands. [...]

CISA orders feds to patch Windows Server WSUS flaw used in attacks

BleepingComputer - 27 October 2025 10:27

The Cybersecurity and Infrastructure Security Agency (CISA) ordered U.S. government agencies to patch a critical-severity Windows Server Update Services (WSUS) vulnerability after adding it to its catalog of security flaws exploited in attacks. [...]

Qilin Targets Windows Hosts With Linux-Based Ransomware

darkreading - 27 October 2025 16:18

The attack by the one of the most impactful RaaS groups active today demonstrates an evasion strategy that can stump defenses not equipped to detect cross-platform threats.

Massive China-Linked Smishing Campaign Leveraged 194,000 Domains

SecurityWeek - 27 October 2025 14:28

The malicious Smishing Triad domains were used to collect sensitive information, including Social Security numbers.

Year-Old WordPress Plugin Flaws Exploited to Hack Websites

SecurityWeek - 27 October 2025 11:46

Roughly 9 million exploit attempts were observed this month as mass exploitation of the critical vulnerabilities recommenced.

Chrome Zero-Day Exploitation Linked to Hacking Team Spyware

SecurityWeek - 27 October 2025 10:33

The threat actor behind Operation ForumTroll used the same toolset typically employed in Dante spyware attacks.

Europol Warns of Rising Threat From Caller ID Spoofing Attacks

Infosecurity Magazine - 27 October 2025 17:00

Europol called for action against caller ID spoofing, linking attacks to significant online fraud