Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 May 2025

Vulnerabilities

‘Ongoing’ Ivanti hijack bug exploitation reaches clouds

The Register - 21 May 2025 02:27

The “ongoing exploitation” of two Ivanti bugs has now extended beyond on-premises environments and hit customers’ cloud instances.

NATO-Flagged Vulnerability Tops Latest VMware Security Patch Batch

SecurityWeek - 20 May 2025 14:57

VMware patches flaws that expose users to data leakage, command execution and denial-of-service attacks. No temporary workarounds available.

Premium WordPress ‘Motors’ theme vulnerable to admin takeover attacks

BleepingComputer - 20 May 2025 16:46

A critical privilege escalation vulnerability has been discovered in the premium WordPress theme Motors, which allows unauthenticated attackers to hijack administrator accounts and take complete control of websites.

Vulnerability Exploitation Probability Metric Proposed by NIST, CISA Researchers

SecurityWeek - 20 May 2025 13:37

The Likely Exploited Vulnerabilities (LEV) equations can help augment KEV- and EPSS-based remediation prioritization.

Threat actors and malware

Hazy Hawk Exploits DNS Records to Hijack CDC, Corporate Domains for Malware Delivery

The Hacker News - 20 May 2025 22:23

A threat actor known as Hazy Hawk has been observed hijacking abandoned cloud resources of high-profile organizations, including Amazon S3 buckets and Microsoft Azure endpoints, by leveraging misconfigurations in the Domain Name System (DNS) records.

Scottish Cyber Coordination Centre

VanHelsing ransomware builder leaked on hacking forum

BleepingComputer - 20 May 2025 16:06

The VanHelsing ransomware-as-a-service operation published the source code for its affiliate panel, data leak blog, and Windows encryptor builder after an old developer tried to sell it on the RAMP cybercrime forum.

Sarcoma Ransomware Unveiled: Anatomy of a Double Extortion Gang

Security Affairs - 20 May 2025 08:37

Cybersecurity Observatory of the Unipegaso's malware lab published a detailed analysis of the Sarcoma ransomware.

Novel Phishing Attack Combines AES With Poisoned npm Packages

darkreading - 20 May 2025 15:00

Researchers discovered a phishing attack in the wild that takes multiple well-tread technologies like open source packages and AES encryption and combines them.

Large Retailers Land in Scattered Spider's Ransomware Web

darkreading - 20 May 2025 16:27

The threat group games IT help desks to gain entry into retailer networks, and signs show it has shifted its attention from the UK to US targets.

UK incidents

Ransomware attack on food distributor spells more pain for UK supermarkets

The Register - 20 May 2025 13:15

More bad news for UK supermarkets with chilled and frozen food distribution business Peter Green Chilled confirming a ransomware attack with customers.