Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 June 2025

Vulnerabilities

WordPress Motors theme flaw mass-exploited to hijack admin accounts

BleepingComputer - 21 June 2025 11:09

Hackers are exploiting a critical privilege escalation vulnerability in the WordPress theme "Motors" to hijack administrator accounts and gain complete control of a targeted site.

Microsoft investigates OneDrive bug that breaks file search

BleepingComputer - 20 June 2025 13:39

Microsoft is investigating a known OneDrive issue that is causing searches to appear blank for some users or return no results even when searching for files they know they've already uploaded.

Linux flaws chain allows Root access across major distributions

Security Affairs - 20 June 2025 10:22

Qualys researchers discovered two local privilege escalation (LPE) vulnerabilities, an attacker can exploit them to gain root privileges on machines running major Linux distributions.

FreeType Zero-Day Found by Meta Exploited in Paragon Spyware Attacks

SecurityWeek - 20 June 2025 11:10

WhatsApp told SecurityWeek that it linked the exploited FreeType vulnerability CVE-2025-27363 to a Paragon exploit.

Threat actors and malware

Cloudflare blocked record-breaking 7.3 Tbps DDoS attack against a hosting provider

Security Affairs - 20 June 2025 21:38

Cloudflare blocked a record 7.3 Tbps DDoS attack in May 2025, 12% greater than its previous peak and 1 Tbps greater than the attack reported by the popular cyber journalist Brian Krebs.

Qilin Ransomware Adds "Call Lawyer" Feature to Pressure Victims for Larger Ransoms

The Hacker News - 20 June 2025 23:05

The threat actors behind the Qilin ransomware-as-a-service (RaaS) scheme are now offering legal counsel for affiliates to put more pressure on victims to pay up, as the cybercrime group intensifies its activity and tries to fill the void left by its rivals.

Scottish Cyber Coordination Centre

Iran confirmed it shut down internet to protect the country against cyberattacks

Security Affairs - 21 June 2025 14:40

Iran confirmed an Internet shutdown to counter Israeli cyberattacks, citing threats to critical infrastructure, and interfere with drone control. Iran experienced a near-total internet blackout on Wednesday as tensions with Israel escalated into the first week of conflict.

UK incidents

Oxford City Council suffers breach exposing two decades of data

BleepingComputer - 22 June 2025 12:17

Oxford City Council warns it suffered a data breach where attackers accessed personally identifiable information from legacy systems.

M&S and Co-op Hacks Classified as Single Cyber Event

Infosecurity Magazine - 20 June 2025 14:30

The recent cyber-attacks on UK retailers Marks & Spencer (M&S) and The Co-op have been publicly linked, with the Cyber Monitoring Centre (CMC) assessing them as a single, combined cyber event.