Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 June 2026

Vulnerabilities

Cisco fixes SD-WAN vManage flaw exploited in zero-day attacks

BleepingComputer - 15 June 2026 14:12

Cisco has released security updates to address a vulnerability in the Catalyst SD-WAN Manager, tracked as CVE-2026-20262, that was exploited in attacks to escalate to root privileges. [...]

Palo Alto Warns of Exploitation of VPN Bypass Exploits (CVE-2026-0257) in PAN-OS Flaw

Security Affairs - 15 June 2026 12:11

Palo Alto Networks warns that attackers are actively exploiting CVE-2026-0257, a PAN-OS flaw that lets unauthorized users bypass authentication and establish VPN connections. Palo Alto Networks has confirmed active exploitation of CVE-2026-0257, a PAN-OS authentication bypass vulnerability affecting GlobalProtect portals and gateways.

CISA Flags LiteSpeed cPanel Plugin Flaw Exploited for Root Privilege Escalation

The Hacker News - 16 June 2026 12:11

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a security flaw impacting LiteSpeed cPanel Plugin to its Known Exploited Vulnerabilities (KEV) catalog, requiring Federal Civilian Executive Branch (FCEB) agencies to apply the fixes by June 18, 2026.

LiteLLM Vulnerability Chain Lets Low-Privilege Users Take Over AI Gateway Servers

The Hacker News - 15 June 2026 23:09

A default low-privilege account on a LiteLLM proxy can climb to full admin and run code on the server by chaining three vulnerabilities, researchers at Obsidian Security disclosedLiteLLM is a widely deployed open-source AI gateway that brokers calls to more than 100 model providers behind one OpenAI-compatible interface.

One-Click Microsoft 365 Copilot Flaw Could Have Let Attackers Steal Emails, Files, and MFA Codes

The Hacker News - 15 June 2026 21:39

A single click on a trusted Microsoft link could have let an attacker pull emails, calendar details, and indexed files out of Microsoft 365 Copilot Enterprise Search.Researchers at Varonis Threat Labs chained three bugs into a one-click exfiltration path they call SearchLeak.

Scottish Cyber Coordination Centre

Threat actors and malware

Supply Chain Attack Hits Popular WordPress Plugins Through Awesome Motive CDN

Security Affairs - 15 June 2026 09:34

Attackers compromised Awesome Motive CDN files, backdooring WordPress sites running OptinMonster, TrustPulse, and PushEngage. Sansec researchers discovered an active supply chain attack hitting WordPress sites running OptinMonster, TrustPulse, and PushEngage, three plugins operated by Awesome Motive, one of the largest WordPress plugin companies in the world.

Chinese Hackers Abused Google Workspace Rules to Steal Research and Defense Emails

The Hacker News - 16 June 2026 02:14

A China-linked espionage group hid inside North American medical, academic, and military research networks for more than a year, quietly stealing sensitive research and defense email.The way in was a backdoor on their REDCap research servers that stole login credentials.

North Korean Hackers Are Turning Developer Tools Into Malware Delivery Channels

The Hacker News - 16 June 2026 02:02

Cybersecurity researchers have flagged two malicious cyber campaigns that exhibit similarities with a persistent North Korean threat cluster known as Contagious Interview (aka Famous Chollima, HexagonalRodent, and Void Dokkaebi).

Council of Europe hacked in ShinyHunters' PeopleSoft heist

The Register - 15 June 2026 20:44

Joins the ranks of Nottingham Uni and 100 other unnamed victims

UK related

UK Government Finds 400+ Vulnerabilities in AI Hackathons

Infosecurity Magazine - 15 June 2026 10:30

Government departments find hundreds of vulnerabilities after testing frontier models