Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 October 2025

Vulnerabilities

TP-Link urges immediate updates for Omada Gateways after critical flaws discovery

Security Affairs - 22 October 2025 18:56

TP-Link warns of critical flaws in Omada gateways across ER, G, and FR models. Users should update firmware immediately to stay secure.

Critical Lanscope Endpoint Manager Bug Exploited in Ongoing Cyberattacks, CISA Confirms

The Hacker News - 23 October 2025 12:07

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a critical security flaw impacting Motex Lanscope Endpoint Manager to its Known Exploited Vulnerabilities (KEV) catalog, stating it has been actively exploited in the wild.

Hackers exploiting critical “SessionReaper” flaw in Adobe Magento

BleepingComputer - 22 October 2025 15:41

Hackers are actively exploiting the critical SessionReaper vulnerability (CVE-2025-54236) in Adobe Commerce (formerly Magento) platforms, with hundreds of attempts recorded.

TARmageddon Flaw in Popular Rust Library Leads to RCE

SecurityWeek - 22 October 2025 16:00

The vulnerability impacts multiple Rust tar parsers, allowing attackers to smuggle additional archive entries.

Chinese Threat Actors Exploit ToolShell SharePoint Flaw Weeks After Microsoft’s July Patch

The Hacker News - 22 October 2025 19:26

Threat actors with ties to China exploited the ToolShell security vulnerability in Microsoft SharePoint to breach a telecommunications company in the Middle East after it was publicly disclosed and patched in July 2025.

Zero-click Dolby audio bug lets attackers run code on Android and Windows devices

Malwarebytes - 22 October 2025 13:00

The bug, tracked as CVE-2025-54957, could let attackers run code via audio files.

Scottish Cyber Coordination Centre

Threat actors and malware

[Iranian hackers targeted over 100 govt orgs with Phoenix backdoor]

BleepingComputer - 22 October 2025 18:19

State-sponsored Iranian hacker group MuddyWater has targeted more than 100 government entities in attacks that deployed version 4 of the Phoenix backdoor.

[PhantomCaptcha targets Ukraine relief groups with WebSocket RAT in October 2025]

Security Affairs - 22 October 2025 21:01

SentinelOne researchers uncovered PhantomCaptcha, a coordinated spear-phishing campaign on October 8, 2025, targeting Ukraine war relief groups, including Red Cross, UNICEF, NRC, and local administrations.

[Scattered Lapsus$ Hunters Signal Shift in Tactics]

Infosecurity Magazine - 22 October 2025 09:30

Scattered Lapsus$ Hunters may be preparing to launch an extortion-as-a-service model, according to Palo Alto Networks.

UK incidents

[Jaguar Land Rover cyber-meltdown tipped to cost the UK almost £2B]

The Register - 22 October 2025 11:29

The Jaguar Land Rover (JLR) cyberattack could end up being the costliest such incident in UK history, billed at an estimated £1.9 billion and affecting over 5,000 organizations.

[UK data regulator defends decision not to investigate MoD Afghan data breach]

The Register - 22 October 2025 08:15

The UK's data protection regulator declined to launch an investigation into a leak at the Ministry of Defence that risked the lives of thousands of Afghans connected with the British Armed Forces.

[UK facing 'most contested and complex' threat in decades, warns GCHQ director]

The Record from Recorded Future News - 22 October 2025 18:45

Speaking at the cybersecurity conference Predict Europe, Anne Keast-Butler — the first woman to lead the cyber and signals intelligence agency GCHQ — said there had been a quadrupling of the most significant cyberattacks over the past year.