Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 May 2026

Vulnerabilities

Copy Fail: New Linux bug enables Root via page-cache corruption

Security Affairs - 30 April 2026 19:23

Xint Code researchers warn of a serious Linux flaw, tracked as CVE-2026-31431 (CVSS score of 7.8), dubbed Copy Fail.

Critical cPanel and WHM bug exploited as a zero-day, PoC now available

BleepingComputer - 30 April 2026 08:40

The critical CVE-2026-41940 authentication bypass vulnerability in cPanel, WHM, and WP Squared is being actively exploited in the wild and has been leveraged in attempts since late February.

Google Fixes CVSS 10 Gemini CLI CI RCE and Cursor Flaws Enable Code Execution

The Hacker News - 30 April 2026 13:37

Google has addressed a maximum severity security flaw in Gemini CLI – the "@google/gemini-cli" npm package and the "google-github-actions/run-gemini-cli" GitHub Actions workflow – that could have allowed attackers to execute arbitrary commands on host systems.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2026-41940 WebPros cPanel & WHM and WP2 (WordPress Squared) Missing Authentication for Critical Function Vulnerability.

SonicWall Urges Immediate Patching of Firewall Vulnerabilities

SecurityWeek - 30 April 2026 15:52

The bugs could be exploited to bypass security controls, access restricted services, and crash firewalls.

Anthropic Unveils Claude Security to Counter AI-Powered Exploit Surge

SecurityWeek - 30 April 2026 19:57

With Mythos signaling a new era of near-instant exploitation, Anthropic positions Claude Security to help defenders keep pace.

Scottish Cyber Coordination Centre

Threat actors and malware

TeamPCP Hits SAP Packages With 'Mini Shai-Hulud' Attack

darkreading - 30 April 2026 22:01

Several npm packages for SAP's cloud application development ecosystem have been compromised as TeamPCP's supply chain attacks broaden.

UK Related

Nearly half of UK businesses pwned last year as phishing keeps doing the job like it's 2005

The Register - 30 April 2026 12:35

Turns out the real problem is not AI but staff still clicking on dodgy emails from 'IT support' Nearly half of UK businesses are still getting breached, and in many cases, the attacker's big breakthrough is an employee clicking "sure, why not" on a fake login page.

UK: Education Sector Faces Surge in Cyber Breaches Despite Stable National Threat Levels

Infosecurity Magazine - 30 April 2026 14:30

The British public education sector has faced the nation's most dramatic increase in cyber breach prevalence over the past year.