Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 April 2026

Vulnerabilities

All supported cPanel versions hit by critical auth bug, now patched

Security Affairs - 29 April 2026 14:55

cPanel released security updates to address a critical authentication vulnerability that could allow attackers to gain unauthorized access to its control panel. The flaw affects all supported versions, raising serious risks for exposed servers.

LiteLLM CVE-2026-42208 SQL Injection Exploited within 36 Hours of Disclosure

The Hacker News - 29 April 2026 12:04

In yet another instance of threat actors quickly jumping on the exploitation bandwagon, a newly disclosed critical security flaw in BerriAI's LiteLLM Python package has come under active exploitation in the wild within 36 hours of the bug becoming public knowledge.

CISA flags data-theft bug in NSA-built OT networking tool

The Register - 29 April 2026 16:35

GrassMarlin leaks sensitive information, provided your targeting phishing skills are sharp enough The Cybersecurity and Infrastructure Security Agency (CISA) is warning anyone who uses GrassMarlin, a tool developed by the National Security Agency (NSA), about a new vulnerability that attackers can use to snoop on sensitive information.

GitHub fixes RCE flaw that gave access to millions of private repos

BleepingComputer - 29 April 2026 09:41

In early March, GitHub patched a critical remote code execution vulnerability (CVE-2026-3854) that could have allowed attackers to access millions of private repositories.

38 Vulnerabilities Found in OpenEMR Medical Software

SecurityWeek - 29 April 2026 10:54

Some of the vulnerabilities discovered by Aisle can be exploited to access and alter sensitive patient information.

Scottish Cyber Coordination Centre

Threat actors and malware

New Wave of DPRK Attacks Uses AI-Inserted npm Malware, Fake Firms, and RATs

The Hacker News - 29 April 2026 21:13

Cybersecurity researchers have discovered malicious code in an npm package after a malicious package as a dependency to the project by Anthropic's Claude Opus large language model (LLM).

Vect 2.0 Ransomware Acts as Wiper, Thanks to Design Error

darkreading - 29 April 2026 16:23

The emerging ransomware has been deployed against victims of the TeamPCP supply chain attacks, but organizations should think twice before paying for a decryptor.