Scottish Cyber Coordination Centre

Daily threat bulletin

14 February 2025

Vulnerabilities

Palo Alto Networks Patches Authentication Bypass Exploit in PAN-OS Software

The Hacker News - 13 February 2025 16:09

Palo Alto Networks has addressed a high-severity security flaw in its PAN-OS software that could result in an authentication bypass.The vulnerability, tracked as CVE-2025-0108, carries a CVSS score of 7.8 out of 10.0.

Rapid7 Flags New PostgreSQL Zero-Day Connected to BeyondTrust Exploitation

SecurityWeek - 13 February 2025 21:03

Rapid7 finds a new zero-day vulnerability in PostgreSQL and links it to chain of attacks against a BeyondTrust Remote Support product.

Exploitation of Old ThinkPHP, OwnCloud Vulnerabilities Surges

SecurityWeek - 13 February 2025 12:22

Threat actors are increasingly exploiting two old vulnerabilities in ThinkPHP and OwnCloud in their attacks.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-57727 SimpleHelp Path Traversal Vulnerability.

Threat actors and malware

whoAMI attacks give hackers code execution on Amazon EC2 instances

BleepingComputer - 13 February 2025 19:35

Security researchers discovered a name confusion attack that allows access to an Amazon Web Services account to anyone that publishes an Amazon Machine Image (AMI) with a specific name. [...]

Hackers Use CAPTCHA Trick on Webflow CDN PDFs to Bypass Security Scanners

The Hacker News - 13 February 2025 21:43

A widespread phishing campaign has been observed leveraging bogus PDF documents hosted on the Webflow content delivery network (CDN) with an aim to steal credit card information and commit financial fraud.

Scottish Cyber Coordination Centre

More victims of China's Salt Typhoon crew emerge: Telcos just now hit via Cisco bugs

The Register - 13 February 2025 19:34

Networks in US and beyond compromised by Beijing's super-snoops pulling off priv-esc attacks China's Salt Typhoon spy crew exploited vulnerabilities in Cisco devices to compromise at least seven devices linked to global telecom providers and other orgs, in addition to its previous victim count....

Chinese APT 'Emperor Dragonfly' Moonlights With Ransomware

darkreading - 13 February 2025 22:32

Pivoting from prior cyber espionage, the threat group deployed its backdoor tool set to ultimately push out RA World malware, demanding $2 million from its victim.