Scottish Cyber Coordination Centre

Daily Threat Bulletin

31 October 2025

Vulnerabilities

U.S. CISA adds XWiki Platform, and Broadcom VMware Aria Operations and VMware Tools flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 31 October 2025 00:14

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added XWiki Platform, and Broadcom VMware Aria Operations and VMware Tools flaws to its Known Exploited Vulnerabilities (KEV) catalog.

New “Brash” Exploit Crashes Chromium Browsers Instantly with a Single Malicious URL

The Hacker News - 30 October 2025 21:15

A severe vulnerability disclosed in Chromium’s Blink rendering engine can be exploited to crash many Chromium-based browsers within a few seconds.

Critical Claroty Authentication Bypass Flaw Opened OT to Attack

darkreading - 30 October 2025 21:29

CVE-2025-54603 gave attackers an opening to disrupt critical operational technology (OT) environments and critical infrastructure, plus steal data from them.

Docker Compose vulnerability opens door to host-level writes – patch pronto

The Register - 30 October 2025 17:27

Windows Desktop installer also fixed after DLL hijack flaw rated 8.8 severity Docker Compose users are being strongly urged to upgrade their versions of the orchestration tool after a researcher uncovered a flaw that could allow attackers to stage path traversal attacks.

Critical Flaws Found in Elementor King Addons Affect 10,000 Sites

Infosecurity Magazine - 30 October 2025 17:45

The King Addons for Elementor plugin contains two flaws allowing unauthenticated file uploads and privilege escalation

Scottish Cyber Coordination Centre

Threat actors and malware

Massive surge of NFC relay malware steals Europeans' credit cards

BleepingComputer - 30 October 2025 17:17

Near-Field Communication (NFC) relay malware has grown massively popular in Eastern Europe, with researchers discovering over 760 malicious Android apps using the technique to steal people's payment card information in the past few months.

Russian Ransomware Gangs Weaponize Open-Source AdaptixC2 for Advanced Attacks

The Hacker News - 30 October 2025 23:10

The open-source command-and-control (C2) framework known as AdaptixC2 is being used by a growing number of threat actors, some of whom are related to Russian ransomware gangs.

PhantomRaven Malware Found in 126 npm Packages Stealing GitHub Tokens From Devs

The Hacker News - 30 October 2025 16:46

Cybersecurity researchers have uncovered yet another active software supply chain attack campaign targeting the npm registry with over 100 malicious packages that can steal authentication tokens, CI/CD secrets, and GitHub credentials from developers' machines.