Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 July 2025

Vulnerabilities

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-2025-6554 - Google Chromium V8 Type Confusion Vulnerability.

Critical Cisco Vulnerability in Unified CM Grants Root Access via Static Credentials

The Hacker News - 03 July 2025 10:54

Cisco has released security updates to address a maximum-severity security flaw in Unified Communications Manager (Unified CM) and Unified Communications Manager Session Management Edition (Unified CM SME) that could permit an attacker to login to a susceptible device as the root user, allowing them to gain elevated privileges.

Chinese Hackers Target France in Ivanti Zero-Day Exploit Campaign

Infosecurity Magazine - 02 July 2025 12:00

The French cybersecurity agency identified Houken, a new Chinese intrusion campaign targeting various industries in France

Forminator plugin flaw exposes WordPress sites to takeover attacks

BleepingComputer - 02 July 2025 12:38

The Forminator plugin for WordPress is vulnerable to an unauthenticated arbitrary file deletion flaw that could enable full site takeover attacks.

Threat actors and malware

ClickFix Spin-Off Attack Bypasses Key Browser Safeguards

darkreading - 02 July 2025 19:00

A new threat vector exploits how modern browsers save HTML files, bypassing Mark of the Web and giving attackers another social-engineering attack for delivering malware.

Hackers Using PDFs to Impersonate Microsoft, DocuSign, and More in Callback Phishing Campaigns

The Hacker News - 02 July 2025 17:15

Cybersecurity researchers are calling attention to phishing campaigns that impersonate popular brands and trick targets into calling phone numbers operated by threat actors.

North Korean Hackers Target Web3 with Nim Malware and Use ClickFix in BabyShark Campaign

The Hacker News - 02 July 2025 23:39

Threat actors with ties to North Korea have been observed targeting Web3 and cryptocurrency-related businesses with malware written in the Nim programming language, underscoring a constant evolution of their tactics.

Cl0p cybercrime gang's data exfiltration tool found vulnerable to RCE attacks

The Register - 02 July 2025 10:38

Security experts have uncovered a hole in Cl0p's data exfiltration tool that could potentially leave the cybercrime group vulnerable to attack....