Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 March 2025

Vulnerabilities

U.S. CISA adds Google Chromium Mojo flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 28 March 2025 00:02

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Google Chromium Mojo sandbox escape vulnerability, tracked as **CVE-2025-2783**, to its Known Exploited Vulnerabilities (KEV) catalog.

Mozilla Patches Critical Firefox Bug Similar to Chrome's Recent Zero-Day Vulnerability

The Hacker News - 28 March 2025 12:14

Mozilla has released updates to address a critical security flaw impacting its Firefox browser for Windows, merely days after Google patched a similar flaw in Chrome that came under active exploitation as a zero-day.

Splunk Patches Dozens of Vulnerabilities

SecurityWeek - 27 March 2025 18:55

Splunk patches high-severity remote code execution and information disclosure flaws in Splunk Enterprise and Secure Gateway App.

The 4 WordPress flaws hackers targeted the most in Q1 2025

BleepingComputer - 27 March 2025 13:29

A new report sheds light on the most targeted WordPress plugin vulnerabilities hackers used in the first quarter of 2025 to compromise sites.

Threat actors and malware

Hackers Repurpose RansomHub's EDRKillShifter in Medusa, BianLian, and Play Attacks

The Hacker News - 27 March 2025 20:40

A new analysis has uncovered connections between affiliates of RansomHub and other ransomware groups like Medusa, BianLian, and Play. The connection stems from the use of a custom tool that's designed to disable endpoint detection and response (EDR) software on compromised hosts, according to ESET.

Scottish Cyber Coordination Centre

New Morphing Meerkat Phishing Kit Mimics 114 Brands Using Victims' DNS Email Records

The Hacker News - 27 March 2025 23:28

Cybersecurity researchers have shed light on a new phishing-as-a-service (PhaaS) platform that leverages the Domain Name System (DNS) mail exchange (MX) records to serve fake login pages that impersonate about 114 brands.

CoffeeLoader Malware Loader Linked to SmokeLoader Operations

Infosecurity Magazine - 27 March 2025 17:45

Newly identified CoffeeLoader uses multiple evasion techniques and persistence mechanisms to deploy payloads and bypass endpoint security.

Infostealer campaign compromises 10 npm packages, targets devs

BleepingComputer - 27 March 2025 17:22

Ten npm packages were suddenly updated with malicious code yesterday to steal environment variables and other sensitive data from developers' systems.

UK Specific

No MFA? Expect Hefty Fines, UK's ICO Warns

Infosecurity Magazine - 27 March 2025 13:45

The ICO's Deputy Commissioner told Infosecurity that organizations that fail to implement MFA and suffer a breach can expect heavy penalties.