Scottish Cyber Coordination Centre

Daily Threat Bulletin

01 April 2025

Vulnerabilities

U.S. CISA adds Cisco Smart Licensing Utility flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 31 March 2025 20:56

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Cisco Smart Licensing Utility vulnerability, tracked as CVE-2024-20439, to its Known Exploited Vulnerabilities (KEV) catalog.

Russian Hackers Exploit CVE-2025-26633 via MSC EvilTwin to Deploy SilentPrism and DarkWisp

The Hacker News - 31 March 2025 23:11

The threat actors behind the zero-day exploitation of a recently-patched security vulnerability in Microsoft Windows have been found to deliver two new backdoors called SilentPrism and DarkWisp. The activity has been attributed to a suspected Russian hacking group called Water Gamayun, which is also known as EncryptHub and LARVA-208.

NCSC Urges Users to Patch Next.js Flaw Immediately

Infosecurity Magazine - 31 March 2025 10:15

The UK's National Cyber Security Agency has called on Next.js users to patch CVE-2025-29927

Threat actors and malware

Threat Actors Deploy WordPress Malware in 'mu-plugins' Directory

SecurityWeek - 31 March 2025 16:05

Sucuri has discovered multiple malware families deployed in the WordPress mu-plugins directory to evade routine security checks.

Phishing platform 'Lucid' behind wave of iOS, Android SMS attacks

BleepingComputer - 31 March 2025 15:49

A phishing-as-a-service (PhaaS) platform named 'Lucid' has been targeting 169 entities in 88 countries using well-crafted messages sent on iMessage (iOS) and RCS (Android).

Scottish Cyber Coordination Centre

Qakbot Resurfaces in Fresh Wave of ClickFix Attacks

darkreading - 31 March 2025 14:57

The previously dormant Qakbot banking Trojan has resurfaced recently as the payload in a wave of attacks on LinkedIn and other social media sites; the attacks leverage the emerging ClickFix technique to trick users into installing malware.