Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 July 2025

Vulnerabilities

U.S. CISA adds Wing FTP Server flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 16 July 2025 01:01

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Wing FTP Server flaw, tracked as CVE-2025-47812, to its Known Exploited Vulnerabilities (KEV) catalog.

Google says 'Big Sleep' AI tool found bug hackers planned to use

The Record from Recorded Future News - 15 July 2025 19:24

According to Google, Big Sleep managed to discover CVE-2025-6965 — a critical security flaw that was "only known to threat actors and was at risk of being exploited".

Threat actors and malware

North Korean XORIndex malware hidden in 67 malicious npm packages

BleepingComputer - 15 July 2025 14:47

North Korean threat actors planted 67 malicious packages in the Node Package Manager (npm) online repository to deliver a new malware loader called XORIndex to developer systems.

Android Malware Konfety evolves with ZIP manipulation and dynamic loading

Security Affairs - 15 July 2025 18:14

A new Konfety Android malware variant uses a malformed ZIP and obfuscation to evade detection, posing as fake apps with no real functionality.

AsyncRAT's Open-Source Code Sparks Surge in Dangerous Malware Variants Across the Globe

The Hacker News - 15 July 2025 17:23

Cybersecurity researchers have charted the evolution of a widely used remote access trojan called AsyncRAT, which was first released on GitHub in January 2019 and has since served as the foundation for several other variants.

Threat Actors Exploit SVG Files in Stealthy JavaScript Redirects

Infosecurity Magazine - 15 July 2025 15:00

A new phishing campaign uses SVG files for JavaScript redirects, bypassing traditional detection methods

Scottish Cyber Coordination Centre

Hyper-Volumetric DDoS Attacks Reach Record 7.3 Tbps, Targeting Key Global Sectors

The Hacker News - 15 July 2025 23:00

Cloudflare on Tuesday said it mitigated 7.3 million distributed denial-of-service (DDoS) attacks in the second quarter of 2025, a significant drop from 20.5 million DDoS attacks it fended off the previous quarter.

New ZuRu Malware Variant Targeting Developers

Security Magazine - 15 July 2025 09:00

A new report reveals new artifacts associated with ZuRu, an Apple macOS malware.

UK incidents

Louis Vuitton says customers in Turkey, South Korea and UK impacted by data breaches

The Record from Recorded Future News - 15 July 2025 15:16

Luxury brand Louis Vuitton said data breaches at its stores in Turkey, South Korea and the United Kingdom exposed the sensitive information of some customers.