Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

31 July 2025

Vulnerabilities

Hackers actively exploit critical RCE in WordPress Alone theme

BleepingComputer - 30 July 2025 14:40

Threat actors are actively exploiting a critical unauthenticated arbitrary file upload vulnerability in the WordPress theme 'Alone,' to achieve remote code execution and perform a full site takeover.

Critical Dahua Camera Flaws Enable Remote Hijack via ONVIF and File Upload Exploits

The Hacker News - 30 July 2025 19:31

Cybersecurity researchers have disclosed now-patched critical security flaws in the firmware of Dahua smart cameras that, if left unaddressed, could allow attackers to hijack control of susceptible devices.

Apple fixed a zero-day exploited in attacks against Google Chrome users

Security Affairs - 30 July 2025 19:09

Apple released security updates to address a high-severity vulnerability, tracked as CVE-2025-6558 (CVSS score of 8.8), that has been exploited in zero-day attacks targeting Google Chrome users.

New Lenovo UEFI firmware updates fix Secure Boot bypass flaws

BleepingComputer - 30 July 2025 11:52

Lenovo is warning about high-severity BIOS flaws that could allow attackers to potentially bypass Secure Boot in all-in-one desktop PC models that use customized Insyde UEFI (Unified Extensible Firmware Interface).

Third of Exploited Vulnerabilities Weaponized Within a Day of Disclosure

Infosecurity Magazine - 30 July 2025 12:45

32.1% of vulnerabilities listed in VulnCheck's Known Exploited Vulnerabilities catalog were weaponized before being detected or within the following day.

Threat actors and malware

FunkSec Ransomware Decryptor Released Free to Public After Group Goes Dormant

The Hacker News - 30 July 2025 22:41

Cybersecurity experts have released a decryptor for a ransomware strain called FunkSec, allowing victims to recover access to their files for free.

ShinyHunters behind Salesforce data theft attacks at Qantas, Allianz Life, and LVMH

BleepingComputer - 30 July 2025 16:52

A wave of data breaches impacting companies like Qantas, Allianz Life, LVMH, and Adidas has been linked to the ShinyHunters extortion group, which has been using voice phishing attacks to steal data from Salesforce CRM instances.

Hackers target Python devs in phishing attacks using fake PyPI site

BleepingComputer - 30 July 2025 15:57

The Python Software Foundation warned users this week that threat actors are trying to steal their credentials in phishing attacks using a fake Python Package Index (PyPI) website.

Scattered Spider Activity Drops Following Arrests, but Others Adopting Group’s Tactics

SecurityWeek - 30 July 2025 14:28

Multiple financially motivated threat actors are targeting backup systems and employing Scattered Spider’s social engineering techniques.