Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 August 2025

Vulnerabilities

Attackers actively exploit critical zero-day in Alone WordPress Theme

Security Affairs - 31 July 2025 17:11

Threat actors are actively exploiting a critical flaw, tracked as CVE-2025-5394 (CVSS score of 9.8), in the “Alone – Charity Multipurpose Non-profit WordPress Theme” to compromise websites.

Honeywell Experion PKS Flaws Allow Manipulation of Industrial Processes

SecurityWeek - 31 July 2025 10:23

Honeywell has patched several critical and high-severity vulnerabilities in its Experion PKS industrial process control and automation product.

Threat actors and malware

Secret Blizzard Deploys Malware in ISP-Level AitM Attacks on Moscow Embassies

The Hacker News - 31 July 2025 23:42

The Russian nation-state threat actor known as Secret Blizzard has been observed orchestrating a new cyber espionage campaign targeting foreign embassies located in Moscow by means of an adversary-in-the-middle (AitM) attack at the Internet Service Provider (ISP) level and delivering a custom malware dubbed ApolloShadow.

CISA unveils free Thorium malware analysis platform

The Record from Recorded Future News - 31 July 2025 16:42

Cyber defenders will now have access to a new free malware analysis platform thanks to the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energys Sandia National Laboratories.

Inside a Real Clickfix Attack: How This Social Engineering Hack Unfolds

BleepingComputer - 31 July 2025 11:05

ClickFix abuses clipboards. FileFix hijacks File Explorer. Both social engineering attacks start in the browser—and end in malware. See how Keep Aware stops these stealthy attacks before they break out of the browser in a run down of a real attack.

Scottish Cyber Coordination Centre

Android Malware Targets Banking Users Through Discord Channels

Infosecurity Magazine - 31 July 2025 16:45

The DoubleTrouble Android banking Trojan has evolved, using Discord for delivery and introducing several new features.

UK incidents

NHS disability equipment provider on brink of collapse a year after cyberattack

The Register - 31 July 2025 13:29

A major supplier of healthcare equipment to the UK's National Health Service and local councils is on the verge of collapse 16 months after falling victim to cyber criminals.