Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 April 2025

Vulnerabilities

Hackers exploit WordPress plugin auth bypass hours after disclosure

BleepingComputer - 10 April 2025 16:11

Hackers started exploiting a high-severity flaw that allows bypassing authentication in the OttoKit (formerly SureTriggers) plugin for WordPress just hours after public disclosure.

An APT group exploited ESET flaw to execute malware

Security Affairs - 10 April 2025 11:47

Kaspersky researchers reported that an APT group, tracked as ToddyCat, has exploited a vulnerability in ESET software to stealthily execute malware, bypassing security. The vulnerability, tracked as CVE-2024-11859, is a DLL Search Order Hijacking issue that potentially allow an attacker with administrator privileges to load a malicious dynamic-link library and execute its code.

OttoKit WordPress Plugin Admin Creation Vulnerability Under Active Exploitation

The Hacker News - 11 April 2025 11:28

A newly disclosed high-severity security flaw impacting OttoKit (formerly SureTriggers) has come under active exploitation within a few hours of public disclosure. The vulnerability, tracked as CVE-2025-3102 (CVSS score: 8.1), is an authorization bypass bug that could permit an attacker to create administrator accounts under certain conditions and take control of susceptible websites.

Juniper Networks Patches Dozens of Junos Vulnerabilities

SecurityWeek - 10 April 2025 14:34

Juniper Networks has patched two dozen vulnerabilities in Junos OS and Junos OS Evolved, and dozens of flaws in Junos Space third-party dependencies.

Threat actors and malware

AkiraBot Targets 420,000 Sites with OpenAI-Generated Spam, Bypassing CAPTCHA Protections

The Hacker News - 10 April 2025 13:45

Cybersecurity researchers have disclosed details of an AI powered platform called AkiraBot that's used to spam website chats, comment sections, and contact forms to promote dubious search engine optimization (SEO) services such as Akira and ServicewrapGO.

Scottish Cyber Coordination Centre

Russian hackers attack Western military mission using malicious drive

BleepingComputer - 10 April 2025 11:23

The Russian state-backed hacking group Gamaredon (aka “Shuckworm”) has been targeting a military mission of a Western country in Ukraine in attacks likely deployed from removable drives.

Threat Actors Use ‘Spam Bombing’ Technique to Hide Malicious Motives

darkreading - 10 April 2025 14:00

Darktrace researchers detailed "spam bombing," a technique in which threat actors bombard targets with spam emails as a pretense for activity like social engineering campaigns.

Infosec experts fear China could retaliate against tariffs with a Typhoon attack

The Register - 10 April 2025 12:00

Scammers are already cashing in with fake invoices for import costs as the trade war between America and China escalates, some infosec and policy experts fear Beijing will strike back in cyberspace.

UK specific

Over 40% of UK Businesses Faced Cybersecurity Breaches in 2024

Infosecurity Magazine - 10 April 2025 14:45

The Cyber Security Breaches Survey 2025 has been released by the UK Home Office and DSIT today, reporting a slight decline in incidents compared to 2024 report.