Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 November 2025

Vulnerabilities

Critical Flaw in Popular React Native NPM Package Exposes Developers to Attacks

SecurityWeek - 04 November 2025 17:10

Arbitrary command/code execution has been demonstrated through the exploitation of CVE-2025-11953 on Windows, macOS and Linux.

Hackers exploit WordPress plugin Post SMTP to hijack admin accounts

BleepingComputer - 04 November 2025 17:46

Threat actors are actively exploiting a critical vulnerability in the Post SMTP plugin installed on more than 400,000 WordPress sites, to take complete control by hijacking administrator accounts.

Critical React Native CLI Flaw Exposed Millions of Developers to Remote Attacks

The Hacker News - 04 November 2025 20:54

Details have emerged about a now-patched critical security flaw in the popular "@react-native-community/cli" npm package that could be potentially exploited to run malicious operating system (OS) commands under certain conditions.

Microsoft Teams Bugs Let Attackers Impersonate Colleagues and Edit Messages Unnoticed

The Hacker News - 04 November 2025 20:30

Cybersecurity researchers have disclosed details of four security flaws in Microsoft Teams that could have exposed users to serious impersonation and social engineering attacks. The vulnerabilities allowed attackers to manipulate conversations, impersonate colleagues, and exploit notifications.

Android Update Patches Critical Remote Code Execution Flaw

SecurityWeek - 04 November 2025 10:24

The November 2025 Android patches resolve two vulnerabilities, both in the platform's System component.

Apple Patches 19 WebKit Vulnerabilities

SecurityWeek - 04 November 2025 12:07

Apple has released iOS 26.1 and macOS Tahoe 26.1 with patches for over 100 vulnerabilities, including critical flaws.

Scottish Cyber Coordination Centre

Windows 10 update bug triggers incorrect end-of-support alerts

BleepingComputer - 04 November 2025 09:31

Microsoft says the October 2025 updates trigger incorrect end-of-support warnings on Windows 10 systems with active security coverage or still under active support.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2025-11371 Gladinet CentreStack and Triofox Files or Directories Accessible to External Parties Vulnerability
CVE-2025-48703 CWP Control Web Panel OS Command Injection Vulnerability

Threat actors and malware

Russian hackers abuse Hyper-V to hide malware in Linux VMs

BleepingComputer - 04 November 2025 10:00

The Russian hacker group Curly COMrades is abusing Microsoft Hyper-V in Windows to bypass endpoint detection and response solutions by creating a hidden Alpine Linux-based virtual machine to run malware.

SesameOp Malware Abuses OpenAI API

SecurityWeek - 04 November 2025 14:38

A component of the newly discovered SesameOp backdoor uses the API to store and relay commands from the C&C server.

DragonForce Cartel Emerges as Conti-Derived Ransomware Threat

Infosecurity Magazine - 04 November 2025 14:45

DragonForce, a ransomware group using Conti's code, has adopted a cartel model to expand and recruit