Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 September 2025

Vulnerabilities

Critical flaw SessionReaper in Commerce and Magento platforms lets attackers hijack customer accounts

Security Affairs - 10 September 2025 21:54

Adobe fixed a critical flaw in its Commerce and Magento Open Source platforms that allows an attacker to take over customer accounts. Adobe addressed a critical vulnerability, tracked as CVE-2025-54236 (aka SessionReaper, CVSS score of 9.1) in its Commerce and Magento Open Source platforms.

Microsoft Patch Tuesday security updates for September 2025 fixed two zero-day flaws

Security Affairs - 10 September 2025 08:48

Microsoft Patch Tuesday security updates for September 2025 fixed 80 vulnerabilities, including two publicly disclosed zero-day flaws. Microsoft Patch Tuesday security updates for September 2025 addressed 80 vulnerabilities in Windows and Windows Components, Office and Office Components, Microsoft Edge (Chromium-based), Azure, Hyper-V, SQL Server, Defender Firewall Service, and Xbox (yup – Xbox!).

How npm Security Collapsed Thanks To a 2FA Exploit

Security Boulevard - 11 September 2025 00:46

Billions (No, that's not a typo, Billions with a capital B) of files were potentially compromised. If you thought Node Package Manager (npm), the JavaScript runtime environment Node.js's default package manager, had finally stopped having serious security problems, you thought wrong.

Cursor Autorun Flaw Lets Repositories Execute Code Without Consent

Infosecurity Magazine - 10 September 2025 13:30

A flaw in the Cursor extension allows unauthorized code execution when opening repositories in Visual Studio

Threat actors and malware

DDoS defender targeted in 1.5 Bpps denial-of-service attack

BleepingComputer - 10 September 2025 19:09

A DDoS mitigation service provider in Europe was targeted in a massive distributed denial-of-service attack that reached 1.5 billion packets per second. [...]

Hackers left empty-handed after massive NPM supply-chain attack

BleepingComputer - 10 September 2025 14:56

The largest supply-chain compromise in the history of the NPM ecosystem has impacted roughly 10% of all cloud environments, but attackers made little profit off it. [...]

CHILLYHELL macOS Backdoor and ZynorRAT RAT Threaten macOS, Windows, and Linux Systems

The Hacker News - 10 September 2025 19:34

Cybersecurity researchers have discovered two new malware families, including a modular Apple macOS backdoor called CHILLYHELL and a Go-based remote access trojan (RAT) named ZynorRAT that can target both Windows and Linux systems.

Watch Out for Salty2FA: New Phishing Kit Targeting US and EU Enterprises

The Hacker News - 10 September 2025 14:30

Phishing-as-a-Service (PhaaS) platforms keep evolving, giving attackers faster and cheaper ways to break into corporate accounts. Now, researchers at ANY.RUN has uncovered a new entrant: Salty2FA, a phishing kit designed to bypass multiple two-factor authentication methods and slip past traditional defenses.

Akira ransomware crims abusing trifecta of SonicWall security holes for extortion attacks

The Register - 10 September 2025 23:41

Patch, turn on MFA, and restrict access to trusted networks…or else Affiliates of the Akira ransomware gang are again exploiting a critical SonicWall vulnerability abused last summer, after a suspected zero-day flaw actually turned out to be related to a year-old bug.…

UK related

Jaguar Land Rover confirms data theft after recent cyberattack

BleepingComputer - 10 September 2025 12:29

Jaguar Land Rover (JLR) confirmed today that attackers also stole “some data” during a recent cyberattack that forced it to shut down systems and instruct staff not to report to work. [...]