Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 March 2025

Vulnerabilities

CISA Warns of Sitecore RCE Flaws; Active Exploits Hit Next.js and DrayTek Devices

The Hacker News - 27 March 2025 12:53

The CISA has added two six-year-old security flaws impacting Sitecore CMS and Experience Platform (XP) to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

- CVE-2019-9874 (CVSS score: 9.8) & CVE-2019-9875 (CVSS score: 8.8) - Deserialization vulnerabilities in the Sitecore.Security.AntiCSRF module that allows an unauthenticated attacker to execute arbitrary code by sending a serialized .NET object in the HTTP POST parameter __CSRFTOKEN

NetApp SnapCenter Flaw Could Let Users Gain Remote Admin Access on Plug-In Systems

The Hacker News - 27 March 2025 12:36

A critical security flaw has been disclosed in NetApp SnapCenter that, if successfully exploited, could allow privilege escalation. SnapCenter is an enterprise-focused software that's used to manage data protection across applications, databases, virtual machines, and file systems, offering the ability to backup, restore, and clone data resources.

New Security Flaws Found in VMware Tools and CrushFTP — High Risk, No Workaround

The Hacker News - 26 March 2025 10:50

Broadcom has issued security patches to address a high-severity security flaw in VMware Tools for Windows that could lead to an authentication bypass. Tracked as CVE-2025-22230, the vulnerability is rated 7.8 on the Common Vulnerability Scoring System (CVSS).

Threat actors and malware

New ReaderUpdate malware variants target macOS users

Security Affairs - 26 March 2025 21:45

SentinelOne researchers warn that multiple versions of the ReaderUpdate malware written in Crystal, Nim, Rust, and Go programming languages, are targeting macOS users.

Scottish Cyber Coordination Centre

EncryptHub Exploits Windows Zero-Day to Deploy Rhadamanthys and StealC Malware

The Hacker News - 26 March 2025 20:23

The threat actor known as EncryptHub exploited a recently-patched security vulnerability in Microsoft Windows as a zero-day to deliver a wide range of malware families, including backdoors and information stealers such as Rhadamanthys and StealC.

StreamElements discloses third-party data breach after hacker leaks data

BleepingComputer - 26 March 2025 15:42

Cloud-based streaming company StreamElements confirms it suffered a data breach at a third-party service provider after a threat actor leaked samples of stolen data on a hacking forum.

New SparrowDoor Backdoor Variants Found in Attacks on U.S. and Mexican Organizations

The Hacker News - 26 March 2025 23:29

The Chinese threat actor known as FamousSparrow has been linked to a cyber attack targeting a trade group in the United States and a research institute in Mexico to deliver its flagship backdoor SparrowDoor and ShadowPad.

MailChimp Under Attack: How Cybercriminals Are Exploiting Email Marketing Platforms

Security Boulevard - 26 March 2025 20:55

Constella have revealed recent cases that involves the abuse of Email Marketing Platforms like MailChimp, whose accounts are being compromised through account takeover (ATO), phishing, and social engineering tactics.

UK Specific

UK fines software provider £3.07 million for 2022 ransomware breach

BleepingComputer - 26 March 2025 21:01

The UK Information Commissioner's Office (ICO) has fined Advanced Computer Software Group Ltd £3.07 million over a 2022 ransomware attack that exposed the sensitive personal data of 79,404 people, including National Health Service (NHS) patients.

UK Government's New Fraud Strategy to Focus on Tech-Enabled Threats

Infosecurity Magazine - 26 March 2025 10:30

The UK government's new fraud minister will today announce plans for a newly expanded fraud strategy.