Scottish Cyber Coordination Centre

Daily threat bulletin

29 January 2025

Vulnerabilities

Actively Exploited Fortinet Zero-Day Gives Attackers Super-Admin Privileges

darkreading - 28 January 2025 12:46

The firewall specialist has patched the security flaw, which was responsible for a series of attacks reported earlier this month that compromised FortiOS and FortiProxy products exposed to the public Internet.

Hackers exploiting flaws in SimpleHelp RMM to breach networks

BleepingComputer - 28 January 2025 17:49

Hackers are believed to be exploiting recently fixed SimpleHelp Remote Monitoring and Management (RMM) software vulnerabilities to gain initial access to target networks. [...]

SonicWall Confirms Exploitation of New SMA Zero-Day

SecurityWeek - 28 January 2025 12:21

SonicWall has confirmed that an SMA 1000 zero-day tracked as CVE-2025-23006 has been exploited in the wild.

Apple Patches Actively Exploited Zero-Day Affecting iPhones, Macs, and More

The Hacker News - 28 January 2025 09:53

Apple has released software updates to address several security flaws across its portfolio, including a zero-day vulnerability that it said has been exploited in the wild.The vulnerability, tracked as CVE-2025-24085, has been described as a use-after-free bug in the Core Media component that could permit a malicious application already installed on a device to elevate privileges.

Zyxel CPE Devices Face Active Exploitation Due to Unpatched CVE-2024-40891 Vulnerability

The Hacker News - 29 January 2025 11:41

Cybersecurity researchers are warning that a critical zero-day vulnerability impacting Zyxel CPE Series devices is seeing active exploitation attempts in the wild.

VMware Warns of High-Risk Blind SQL Injection Bug in Avi Load Balancer

SecurityWeek - 28 January 2025 21:49

VMware warns that a malicious user with network access may be able to use specially crafted SQL queries to gain database access.

Scottish Cyber Coordination Centre

Threat actors and malware

New Apple CPU side-channel attacks steal data from browsers

BleepingComputer - 28 January 2025 14:00

A team of security researchers has disclosed new side-channel vulnerabilities in modern Apple processors that could steal sensitive information from web browsers. [...]

Phishing Campaign Baits Hook With Malicious Amazon PDFs

darkreading - 28 January 2025 22:32

In their discovery, researchers found 31 PDF files linking to these phishing websites, none of which have been yet submitted to VirusTotal.

Lynx Ransomware Group Unveiled with Sophisticated Affiliate Program

Infosecurity Magazine - 28 January 2025 17:30

Group-IB researchers have exposed the highly organized affiliate platform and sophisticated operations of the Lynx Ransomware-as-a-Service group

Chinese AI platform DeepSeek faced a “large-scale” cyberattack

Security Affairs - 28 January 2025 09:36

Chinese AI company DeepSeek has disabled registrations for its DeepSeek-V3 chat platform following a “large-scale” cyberattack. DeepSeek has designed a new AI platform that quickly gained attention over the past week primarily due to its significant advancements in artificial intelligence and its impactful applications across various industries.

UK related

Spending watchdog blasts UK govt over sloth-like cyber resilience progress

The Register - 29 January 2025 08:24

Think government cybersecurity is bad? Guess again. It’s alarmingly so The UK government is significantly behind on its 2022 target to harden systems against cyberattacks by 2025, with a new report from the spending watchdog suggesting it may not achieve this goal even by 2030.

Engineering giant Smiths Group discloses security breach

BleepingComputer - 28 January 2025 13:28

London-based engineering giant Smiths Group disclosed a security breach after unknown attackers gained access to the company’s systems. [...]