Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 November 2025

Vulnerabilities

Critical Triofox bug exploited to run malicious payloads via AV configuration

Security Affairs - 11 November 2025 08:28

Google's Mandiant researchers spotted threat actors exploiting a now-patched Triofox flaw, tracked as CVE-2025-12480 (CVSS score of 9.1) that allows them to bypass authentication to upload and run remote access tools via the platform's antivirus feature.

Microsoft Patch Tuesday security updates for November 2025 fixed an actively exploited Windows Kernel bug

Security Affairs - 12 November 2025 07:14

Microsoft fixed over 60 flaws, including an actively exploited Windows kernel zero-day, in its latest Patch Tuesday updates. Impacted services include Windows and Windows Components, Office and Office Components, Microsoft Edge (Chromium-based), Azure Monitor Agent, Dynamics 365, Hyper-V, SQL Server, and the Windows Subsystem for Linux.

SAP fixes hardcoded credentials flaw in SQL Anywhere Monitor

BleepingComputer - 11 November 2025 11:38

SAP has released its November security updates that address multiple security vulnerabilities, including a maximum severity flaw in the non-GUI variant of the SQL Anywhere Monitor and a critical code injection issue in the Solution Manager platform.

Adobe Patches 29 Vulnerabilities

SecurityWeek - 11 November 2025 22:20

Adobe has fixed InDesign, InCopy, Photoshop, Illustrator, Pass, Substance 3D Stager, and Format Plugins vulnerabilities.

Synology fixes BeeStation zero-days demoed at Pwn2Own Ireland

BleepingComputer - 11 November 2025 18:34

Synology has addressed a critical-severity remote code execution (RCE) vulnerability in BeeStation products that was demonstrated at the recent Pwn2Own hacking competition.

Scottish Cyber Coordination Centre

Threat actors and malware

Fantasy Hub: Russian-sold Android RAT boasts full device espionage as MaaS

Security Affairs - 11 November 2025 16:21

Researchers uncovered Fantasy Hub, a Russian-sold Android RAT offered as Malware-as-a-Service, enabling spying, device control, and data theft via Telegram. The malware allows operators to take over infected devices, gathering SMS messages, contacts, call logs, images, and videos.

GootLoader Is Back, Using a New Font Trick to Hide Malware on WordPress Sites

The Hacker News - 11 November 2025 22:14

The malware known as GootLoader has resurfaced yet again after a brief spike in activity earlier this March, according to new findings from Huntress. The cybersecurity company said it observed three GootLoader infections since October 27, 2025, out of which two resulted in hands-on keyboard intrusions with domain controller compromise taking place within 17 hours of initial infection.

North Korean spies turn Google's Find Hub into remote-wipe weapon

The Register - 11 November 2025 17:26

KONNI espionage crew covertly abused Google's Find My Device feature to remotely factory-reset Android phones North Korean state-backed spies have found a new way to torch evidence of their own cyber-spying – by hijacking Google's "Find Hub" service to remotely wipe Android phones belonging to their South Korean targets.

Qilin Ransomware Activity Surges as Attacks Target Small Businesses

Infosecurity Magazine - 11 November 2025 17:00

Qilin group ransomware incidents have surged in SMBs, exploiting security gaps and collaborating with Scattered Spider threat group.

UK incidents

Cyber insurers paid out over twice as much for UK ransomware attacks last year

The Register - 11 November 2025 12:04

Massive increase in policy claims. The number of successful cyber insurance claims made by UK organizations shot up last year, according to the latest figures from the industry's trade association.