Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 November 2025

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-21042 Samsung Mobile Devices Out-of-Bounds Write Vulnerability

Popular JavaScript library expr-eval vulnerable to RCE flaw

BleepingComputer - 10 November 2025 14:32

A critical vulnerability in the popular expr-eval JavaScript library, with over 800,000 weekly downloads on NPM, can be exploited to execute code remotely through maliciously crafted input.

Hackers Exploiting Triofox Flaw to Install Remote Access Tools via Antivirus Feature

The Hacker News - 11 November 2025 03:19

Google's Mandiant Threat Defense on Monday said it discovered n-day exploitation of a now-patched security flaw in Gladinet's Triofox file-sharing and remote access platform. The critical vulnerability, tracked as CVE-2025-12480 (CVSS score: 9.1), allows an attacker to bypass authentication and access the configuration pages, resulting in the upload and execution of arbitrary payloads.

Runc Vulnerabilities Can Be Exploited to Escape Containers

SecurityWeek - 10 November 2025 15:29

The flaws tracked as CVE-2025-31133, CVE-2025-52565, and CVE-2025-52881 have been patched.

Threat actors and malware

APT37 hackers abuse Google Find Hub in Android data-wiping attacks

BleepingComputer - 10 November 2025 20:46

North Korean hackers from the KONNI activity cluster are abusing Google's Find Hub tool to track their targets' GPS positions and trigger remote factory resets of Android devices.

Scottish Cyber Coordination Centre

Quantum Route Redirect PhaaS targets Microsoft 365 users worldwide

BleepingComputer - 10 November 2025 17:29

A new phishing automation platform named Quantum Route Redirect is using around 1,000 domains to steal Microsoft 365 users' credentials.

Large-Scale ClickFix Phishing Attacks Target Hotel Systems with PureRAT Malware

The Hacker News - 10 November 2025 15:41

Cybersecurity researchers have called attention to a massive phishing campaign targeting the hospitality industry that lures hotel managers to ClickFix-style pages and harvest their credentials by deploying malware like PureRAT.

Nearly 30 Alleged Victims of Oracle EBS Hack Named on Cl0p Ransomware Site

SecurityWeek - 10 November 2025 12:46

The Cl0p website lists major organizations such as Logitech, The Washington Post, Cox Enterprises, Pan American Silver, LKQ Corporation, and Copeland.

UK incidents

Allianz UK joins growing list of Clop's Oracle E-Business Suite victims

The Register - 10 November 2025 10:48

Allianz UK confirms it was one of the many companies that fell victim to the Clop gang's Oracle E-Business Suite (EBS) attack after criminals reported that they had attacked a subsidiary.