



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

3 December 2025

Vulnerabilities

[Google's latest Android security update fixes two actively exploited flaws](#)

Security Affairs - 02 December 2025 11:23

Google's new Android update patches 107 vulnerabilities, including two already exploited in the wild, across system, kernel, and major vendor components.

[CISA Adds Two Known Exploited Vulnerabilities to Catalog](#)

CISA Advisories -

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

CVE-2025-48572 Android Framework Privilege Escalation Vulnerability

CVE-2025-48633 Android Framework Information Disclosure Vulnerability

[Undetected Firefox WebAssembly Flaw Put 180 Million Users at Risk](#)

Security Boulevard - 02 December 2025 19:30

Cybersecurity startup Aisle discovered a subtle but dangerous coding error in a Firefox WebAssembly implementation that went undetected for six months despite being shipped with a regression testing capability created by Mozilla to find such a problem.

[Vulnerability in OpenAI Coding Agent Could Facilitate Attacks on Developers](#)

SecurityWeek - 02 December 2025 13:02

The Codex CLI vulnerability tracked as CVE-2025-61260 can be exploited for command execution.

Threat actors and malware

[Microsoft Defender portal outage disrupts threat hunting alerts](#)

BleepingComputer - 02 December 2025 12:10

Microsoft is working to mitigate an ongoing incident that has been blocking access to some Defender XDR portal capabilities for the past 10 hours.



Scottish
Cyber
Coordination
Centre

MuddyWater strikes Israel with advanced MuddyViper malware

Security Affairs - 02 December 2025 16:19

ESET researchers uncovered a new MuddyWater campaign targeting Israeli organizations and one confirmed Egyptian target. The Iran-linked APT group MuddyWater (aka SeedWorm, TEMP.Zagros, Mango Sandstorm, TA450, and Static Kitten) deployed custom tools to evade defenses and maintain persistence.

Shai-Hulud 2.0 NPM malware attack exposed up to 400,000 dev secrets

BleepingComputer - 02 December 2025 15:06

The second Shai-Hulud attack last week exposed around 400,000 raw secrets after infecting hundreds of packages in the NPM (Node Package Manager) registry and publishing stolen data in 30,000 GitHub repositories.

ShadyPanda's Seven-Year Campaign Infects 4.3M Chrome and Edge Users

Infosecurity Magazine - 02 December 2025 16:10

Infected 4.3 million Chrome and Edge users via extensions; ShadyPanda exploited browser marketplaces.

UK incidents

Kensington and Chelsea confirms IT outage was a data breach after all

The Register - 02 December 2025 16:18

Borough says attackers copied 'historical' info as three-council cyber woes drag on
Kensington and Chelsea Council has admitted that data was quietly lifted from its systems during last week's cyber meltdown, confirming that the outage was not just an IT faceplant but a bona fide data breach.