Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 December 2025

Vulnerabilities

Google Patches 107 Android Flaws, Including Two Framework Bugs Exploited in the Wild

The Hacker News - 02 December 2025 13:47

Google on Monday released monthly security updates for the Android operating system, including two vulnerabilities that it said have been exploited in the wild.The patch addresses a total of 107 security flaws spanning different components, including Framework, System, Kernel, as well as those from Arm, Imagination Technologies, MediaTek, Qualcomm, and Unison.

CISA Warns of ScadaBR Vulnerability After Hacktivist ICS Attack

SecurityWeek - 01 December 2025 12:06

CISA has added CVE-2021-26829 to its Known Exploited Vulnerabilities (KEV) catalog.

Threat actors and malware

Glassworm malware returns in third wave of malicious VS Code packages

BleepingComputer - 01 December 2025 17:08

The Glassworm campaign, which first emerged on the OpenVSX and Microsoft Visual Studio marketplaces in October, is now in its third wave, with 24 new packages added on the two platforms. [...]

ShadyPanda browser extensions amass 4.3M installs in malicious campaign

BleepingComputer - 01 December 2025 11:01

A long-running malware operation known as “ShadyPanda” has amassed over 4.3 million installations of seemingly legitimate Chrome and Edge browser extensions that evolved into malware. [...]

Emerging Android threat ‘Albiriox’ enables full On-Device Fraud

Security Affairs - 01 December 2025 11:38

Albiriox is new Android MaaS malware enabling on-device fraud and real-time control. It targets 400+ banking, fintech, crypto, and payment apps. Albiriox is a new Android malware sold under a malware-as-a-service model on Russian-speaking cybercrime forums.

Tomiris Shifts to Public-Service Implants for Stealthier C2 in Attacks on Government Targets

Scottish Cyber Coordination Centre

The Hacker News - 01 December 2025 11:37

The threat actor known as Tomiris has been attributed to attacks targeting foreign ministries, intergovernmental organizations, and government entities in Russia with an aim to establish remote access and deploy additional tools.

Shai-hulud 2.0 Variant Threatens Cloud Ecosystem

darkreading - 01 December 2025 12:10

The latest attack from the self-replicating npm-package poisoning worm can also steal credentials and secrets from AWS, Google Cloud Platform, and Azure.