Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 June 2026

Vulnerabilities

U.S. CISA adds Android and Linux Kernel flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 03 June 2026 11:43

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Windows Shell and ConnectWise ScreenConnect flaws to its Known Exploited Vulnerabilities (KEV) catalog.

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-2026-45247 Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability

Organizations Warned of Exploited Linux Kernel Vulnerability

SecurityWeek - 03 June 2026 12:56

An improper authentication bug allows attackers to escalate their privileges and escape containers.

Google Patches Actively Exploited Android Flaw Affecting Millions of Devices

Security Affairs - 03 June 2026 10:44

Google has released its June 2026 Android security updates, fixing 124 vulnerabilities across the mobile operating system. One flaw, tracked as CVE-2025-48595 (CVSS score of 8.4) stands out from the rest because it is already being exploited in the wild.

Acer working to patch max severity zero-days in Wave 7 routers

BleepingComputer - 03 June 2026 08:35

Acer is working to address two maximum-severity zero-day vulnerabilities affecting its Wave 7 mesh routers.

Microsoft 365 Android Apps Let Any App Steal Account Tokens via Leftover Debug Flag

The Hacker News - 03 June 2026 21:26

A development flag left switched on in production builds of several Microsoft 365 Android apps disabled the check that limits account-token sharing to trusted Microsoft apps.

Scottish Cyber Coordination Centre

Threat actors and malware

Chinese hackers use new Atlas RAT malware in European cyberattacks

BleepingComputer - 03 June 2026 18:45

A Chinese-speaking cybercrime group has expanded its targeting to the European space, deploying previously undocumented malware and the Atlas backdoor.

Google DoubleClick Abused in New Malspam Campaign to Deliver DesckVB RAT

The Hacker News - 03 June 2026 22:59

Cybersecurity researchers have flagged a new malspam campaign that makes use of Google's DoubleClick domain as a way to evade detection and ultimately deliver a remote access trojan (RAT) named DesckVB RAT.

One-Click GitHub Dev Attack Lets Attackers Steal Full GitHub OAuth Tokens

The Hacker News - 03 June 2026 19:28

Cybersecurity researchers have disclosed a one-click attack via Microsoft Visual Studio Code (VS Code) that makes it possible to steal a user's GitHub token. "Just by clicking a link, it's possible for an attacker to steal a GitHub token that can read and write to your repos, including private ones.

Attackers Use AI to Automate EDR Evasion Testing

darkreading - 03 June 2026 22:34

Python scripts were used to test malware against endpoint detection and response agents from Sophos, CrowdStrike, and Windows Defender.

Infostealers are becoming the go-to phishing payload

Malwarebytes - 03 June 2026 09:59

Cybercriminals prefer infostealers to traditional phishing techniques because they reduce friction, scale well, and are widely available.