Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 May 2026

Vulnerabilities

Critical Apache HTTP/2 Flaw (CVE-2026-23918) Enables DoS and Potential RCE

The Hacker News - 05 May 2026 22:49

The Apache Software Foundation (ASF) has released security updates to address several security vulnerabilities in the HTTP Server, including a severe vulnerability that could potentially lead to remote code execution (RCE).

Critical Android vulnerability CVE-2026-0073 fixed by Google

Security Affairs - 05 May 2026 15:06

Google patched a critical Android flaw (CVE-2026-0073) that lets attackers run code remotely without user action. Google released a security update for Android to address a critical remote code execution flaw, tracked as CVE-2026-0073, in the System component.

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-2026-31431 Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability

Palo Alto Networks to Patch Zero-Day Exploited to Hack Firewalls

SecurityWeek - 06 May 2026 05:46

CVE-2026-0300 affects the Captive Portal service of PAN-OS software on PA and VM series firewalls.

WhatsApp Discloses File Spoofing, Arbitrary URL Scheme Vulnerabilities

SecurityWeek - 05 May 2026 10:01

The vulnerabilities were reported to Meta through its bug bounty program and were patched with updates released earlier this year.

MetInfo CMS CVE-2026-29014 Exploited for Remote Code Execution Attacks

The Hacker News - 05 May 2026 18:26

Threat actors are actively exploiting a critical security flaw impacting an open-source content management system (CMS) known as MetInfo, according to new findings from VulnCheck. The vulnerability in question is CVE-2026-29014 (CVSS score: 9.8), a code injection flaw that could result in arbitrary code execution.

Scottish Cyber Coordination Centre

NCSC Warns of an AI-Fuelled "Vulnerability Patch Wave"

Infosecurity Magazine - 05 May 2026 10:40

The UK's National Cyber Security Centre is urging organizations to prepare for glut of new software updates.

Threat actors and malware

Microsoft warns of global campaign stealing auth tokens from 35K users

Security Affairs - 05 May 2026 10:10

Microsoft disclosed a major phishing campaign that targeted over 35,000 users across 26 countries in mid-April 2026. Attackers used fake "code of conduct" emails sent through legitimate platforms to trick recipients into visiting bogus sites.

New stealthy Quasar Linux malware targets software developers

BleepingComputer - 05 May 2026 19:01

A previously undocumented Linux implant named Quasar Linux (QLNX) is targeting developers' systems with a mix of rootkit, backdoor, and credential-stealing capabilities.

DAEMON Tools trojanized in supply-chain attack to deploy backdoor

BleepingComputer - 05 May 2026 16:21

Hackers trojanized installers for the DAEMON Tools software and since April 8, delivered a backdoor to thousands of systems that downloaded the product from the official website.

China-Linked UAT-8302 Targets Governments Using Shared APT Malware Across Regions

The Hacker News - 05 May 2026 20:49

A sophisticated China-nexus advanced persistent threat (APT) group has been attributed to attacks targeting government entities in South America since at least late 2024 and government agencies in southeastern Europe in 2025.