Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 June 2026

Vulnerabilities

CC-4792 - Exploitation of Authentication Bypass Vulnerability in Check Point VPN

NHS Digital - 08 June 2026 13:58

Severity: High Successful exploitation of CVE-2026-50751 could allow an attacker to establish a VPN session without a valid password Successful exploitation of CVE-2026-50751 could allow an attacker to establish a VPN session without a valid password Updated: 08 Jun 2026

Gogs patches critical zero-day enabling remote code execution

BleepingComputer - 08 June 2026 13:18

Gogs has patched a critical security zero-day flaw that can allow attackers to compromise Internet-facing instances and access any repositories (including private ones). [...]

Critical UniFi OS bug lets hackers gain root without authentication

BleepingComputer - 08 June 2026 12:51

Attackers can chain three already fixed vulnerabilities in the Ubiquiti UniFi OS server to execute remote code with root privileges and without authentication. [...]

Everest Forms Pro WordPress Flaw is Handing Attackers Admin Access

Security Affairs - 08 June 2026 15:11

Hackers exploit CVE-2026-3300 in Everest Forms Pro to inject PHP via form fields, creating rogue admin accounts. 29,300 attempts blocked. Researcher h0xilo submitted a flaw in Everest Forms Pro for WordPress, tracked as CVE-2026-3300, to Wordfence's bug bounty program and earned $325 for it.

Google Patches 429 Chrome Vulnerabilities in Major Browser Update

Security Boulevard - 08 June 2026 17:36

Google has patched 429 vulnerabilities in its Chrome browser, an unusually large update for a stable Chrome release. Chrome 149 was released with fixes for security flaws affecting the browser's rendering, graphics, networking and extension components.

Mythos Found 10,000 Vulnerabilities. The Bigger Challenge Is Fixing Them

Security Boulevard - 08 June 2026 15:00

You don't need an AI-scale fortune to be Mythos ready. You need automated, policy-driven remediation that can close the gap between vulnerability discovery and verified fixes. Keep reading for a practical 30-60-90 day playbook to get there.

Scottish Cyber Coordination Centre

Meta AI Bug Exposes Over 20,000 Instagram Accounts

Infosecurity Magazine - 08 June 2026 09:00

Meta confirms an AI tool vulnerability led to unauthorized access to Instagram accounts after a failure in email verification during password reset

Critical Zcash Vulnerability Found and Fixed

Schneier on Security - 08 June 2026 18:06

If you're a user—owner?—of this cryptocurrency, this is important:On May 29, the security researcher Taylor Hornby found a critical vulnerability in Zcash Orchard privacy pool using Claude Opus 4.8. The Zcash team hired Hornby specifically to look for this kind of issue. He found one fast enough to be embarrassing.

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-2026-28318 SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability

Threat actors and malware

VS Code Adds 2-Hour Extension Auto-Update Delay to Limit Supply Chain Attacks

The Hacker News - 08 June 2026 12:38

Microsoft has announced that Visual Studio Code (VS Code) will apply a two-hour delay before extensions for the integrated development environment (IDE) are updated automatically to a newer version in an attempt to tackle software supply chain threats.

WhatsApp Catches Spyware Firm NSO Defying No-Hacking Court Order

SecurityWeek - 08 June 2026 14:23

The Meta-owned communications app is filing a federal court contempt order against NSO.

Silent Ransom Group Uses DNS Fast Flux in Attacks

SecurityWeek - 08 June 2026 11:31

Focusing on hacking law firms in the US, the ransomware group relies on fast flux to hide its C&C infrastructure.