Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 June 2026

Vulnerabilities

CC-4791 - Cisco Releases Security Advisory for Critical Vulnerability in Unified Communications Manager

NHS Digital - 04 June 2026 14:14

Severity: Medium If exploited, CVE-2026-20230 could allow a remote unauthenticated attacker to elevate privileges to root If exploited, CVE-2026-20230 could allow a remote unauthenticated attacker to elevate privileges to root Updated: 04 Jun 2026

U.S. CISA adds Mirasvit Full Page Cache Warmer flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 04 June 2026 18:10

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Mirasvit Full Page Cache Warmer flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Mirasvit Full Page Cache Warmer flaw, tracked as CVE-2026-45247 (CVSS ver 4.0 score of 9.3), to its Known Exploited Vulnerabilities (KEV) catalog.

Gamaredon Uses WinRAR Vulnerability to Launch Modular Spy Campaign on Ukrainian Targets

Security Affairs - 04 June 2026 11:53

Gamaredon exploits a WinRAR flaw to drop modular, nearly fileless malware on Ukrainian targets, hiding payloads in Windows streams and resolving C2s via Telegram. Sekoia's Threat Detection & Research team dropped a YARA rule in late December 2025 to hunt for new initial access vectors, and by January 2026 it had already generated a dozen [...]

Everest Forms Pro Vulnerability Allows Remote Code Execution on WordPress Sites

Infosecurity Magazine - 04 June 2026 17:15

Critical Everest Forms Pro RCE flaw exploited to create rogue WordPress admin accounts

Infosecurity Europe: Mythos Outperforms GPT5.5 on Google Chrome Vulnerability Exploits, Says New Benchmark

Infosecurity Magazine - 04 June 2026 14:00

A Bugcrowd researcher has unveiled ExploitBench, an independent benchmark of AI models for vulnerability exploitation

Threat actors and malware

Scottish Cyber Coordination Centre

Software supply chain attacks: check your dependencies

NCSC - 04 June 2026 13:00

Attackers are compromising open-source packages to spread malware. Cyber defenders are asked to review dependencies to reduce risks

New IronWorm malware hits 36 packages in npm supply-chain attack

BleepingComputer - 04 June 2026 12:25

A new supply-chain attack has infected 36 packages on the Node Package Manager (npm) index with infostealer malware called IronWorm. [...]

China-Linked TA4922 Expands Phishing Attacks to U.K., Germany, Italy, and South Africa

The Hacker News - 04 June 2026 18:52

A new China-linked cybercrime group known as TA4922 has expanded its targeting focus to target European organizations in the U.K., Germany, Italy, and South Africa.

Fake Sites Mimicking Open-Source Tools Rank High on Google to Deliver Malware via TDS

The Hacker News - 04 June 2026 16:21

Cybersecurity researchers have flagged a large-scale operation that impersonates open-source and freeware projects to funnel unsuspecting users through a Traffic Distribution System (TDS) and deliver malware families like Remus Stealer, AnimateClipper, and the SessionGate framework

HTTP/2 Bomb: A New Denial-of-Service Technique Targeting Web Servers

Security Boulevard - 04 June 2026 17:15

A newly discovered denial-of-service (DoS) technique dubbed HTTP/2 Bomb has drawn significant attention across the security industry due to its ability to exhaust server memory and render web services unavailable within seconds. The attack was publicly disclosed in June 2026 by California-based security research company Calif.