Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 June 2026

Vulnerabilities

Cisco Unified CM Flaw CVE-2026-20230 Actively Exploited in the Wild

Security Affairs - 24 June 2026 14:10

Attackers exploit Cisco Unified CM flaw (CVE-2026-20230) allowing unauth HTTP requests to trigger SSRF, write files, and gain root access.

Mandiant reveals how Cisco SD-WAN zero-day attacks gained root access

BleepingComputer - 24 June 2026 18:29

New details have been revealed on how hackers exploited a Cisco Catalyst SD-WAN vulnerability tracked as CVE-2026-20245 in zero-day attacks to create rogue root accounts on targeted devices.

U.S. CISA adds Ubiquiti UniFi OS and Lantronix EDS5000 plugin flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 24 June 2026 11:00

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Ubiquiti UniFi OS and Lantronix EDS5000 flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Critical Ubiquiti Vulnerabilities in Attackers' Crosshairs

SecurityWeek - 24 June 2026 13:32

The flaws allow remote, unauthenticated attackers to make system changes, access underlying accounts, and inject commands.

Cordyceps CI/CD Flaws Expose 300+ GitHub Repositories to Supply-Chain Attacks

The Hacker News - 24 June 2026 19:18

Cybersecurity researchers have flagged a new class of CI/CD workflow weakness that allows attackers to hijack workflows and compromise open-source supply chains. The "critical exploitable pattern" has been codenamed Cordyceps by Novee Security.

Threat actors and malware

Malicious Edge extension abuses Native Messaging as bridge to malware

BleepingComputer - 24 June 2026 17:58

A malicious Microsoft Edge extension dubbed 'Edgecution' has been used in a ransomware attack to escape the browser sandbox and deploy a Python-based backdoor.

Scottish Cyber Coordination Centre

Europol Disrupts StealC and Amadey Malware Infrastructure in Operation Endgame

Security Affairs - 24 June 2026 19:43

Between June 15 and 19, 2026, Europol coordinated a two-week law enforcement operation involving agencies from Canada, Denmark, Germany, the Netherlands, the UK, and the US, alongside private firms like Microsoft, Bitdefender, IBM X-Force, Proofpoint, Infoblox, Shadowserver, Orange Cyberdefense, and a dozen other private partners.

New 'Mistic' RAT Opens Door to Several Ransomware Families

SecurityWeek - 24 June 2026 12:42

Mistic is used by Woodgnat, an initial access broker working with Qilin, Interlock, Rhysida, Akira, 8Base, and Black Basta.