Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 April 2026

Vulnerabilities

CISA orders feds to patch BlueHammer flaw exploited as zero-day

BleepingComputer - 23 April 2026 08:05

CISA has ordered U.S. federal agencies to patch a Microsoft Defender privilege escalation flaw (dubbed BlueHammer) that has been exploited in zero-day attacks.

Apple Fixes iOS Flaw That Let FBI Recover Deleted Signal Messages

The Hacker News - 23 April 2026 14:36

The vulnerability, tracked as CVE-2026-28950 (CVSS score: N/A), has been described as a logging issue that has been addressed with improved data redaction.

Recent Microsoft Defender Vulnerability Exploited as Zero-Day

SecurityWeek - 23 April 2026 09:00

The flaw allows attackers to access the SAM database, extract NTLM hashes, and gain System privileges.

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-2026-39987 Marimo Remote Code Execution Vulnerability

Threat actors and malware

New Checkmarx supply-chain breach affects KICS analysis tool

BleepingComputer - 23 April 2026 13:05

Hackers have compromised Docker images, VSCode and Open VSX extensions for the Checkmarx KICS analysis tool to harvest sensitive data from developer environments.

Executive Summary: Defending against China-nexus covert networks of compromised devices

NCSC - 23 April 2026 13:00

Organisations should map and baseline their edge device traffic, especially VPN and remote access connections, and adopt dynamic threat feed filtering that includes known covert network indicators.

Scottish Cyber Coordination Centre

RAMP Uncovered: Anatomy of Russia's Ransomware Marketplace

Security Affairs - 23 April 2026 11:16

Leaked data from RAMP reveals Russia's ransomware ecosystem, analyzing 1,732 threads, 7,707 users, and 340,000 IP records from the forum.

Trigona ransomware attacks use custom exfiltration tool to steal data

BleepingComputer - 23 April 2026 15:59

Recently observed Trigona ransomware attacks are using a custom, command-line tool to steal data from compromised environments faster and more efficiently.

'Zealot' Shows What AI's Capable of in Staged Cloud Attack

darkreading - 23 April 2026 11:00

The proof of concept revealed AI-based attacks unfold too fast for human defenders to respond, and that AI evinced more autonomous behavior than expected.

Cyber-Attacks Surge 63% Annually in Education Sector

Infosecurity Magazine - 23 April 2026 11:30

Quorum Cyber report finds higher and further education institutions experienced 63% increase in attacks over a year