Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 March 2026

Vulnerabilities

CISA Flags Actively Exploited Wing FTP Vulnerability Leaking Server Paths

The Hacker News - 17 March 2026 11:53

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a medium-severity security flaw impacting Wing FTP to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Critical Unpatched Telnetd Flaw (CVE-2026-32746) Enables Unauthenticated Root RCE via Port 23

The Hacker News - 18 March 2026 11:36

Cybersecurity researchers have disclosed a critical security flaw impacting the GNU InetUtils telnet daemon (telnetd) that could be exploited by an unauthenticated remote attacker to execute arbitrary code with elevated privileges.

Apple pushes first Background Security Improvements update to fix WebKit flaw

BleepingComputer - 17 March 2026 22:06

Apple has released its first Background Security Improvements update to fix a WebKit flaw tracked as CVE-2026-20643 on iPhones, iPads, and Macs without requiring a full operating system upgrade.

Threat actors and malware

RondoDox botnet expands arsenal targeting 174 flaws, and hits 15,000 daily exploit attempts

Security Affairs - 17 March 2026 16:01

RondoDox botnet is ramping up attacks, targeting 174 vulnerabilities with up to 15,000 daily exploitation attempts in a more focused and strategic campaign.

GlassWorm malware hits 400+ code repos on GitHub, npm, VSCode, OpenVSX

BleepingComputer - 17 March 2026 18:42

The GlassWorm supply-chain campaign has returned with a new, coordinated attack that targeted hundreds of packages, repositories, and extensions on GitHub, npm, and VSCode/OpenVSX extensions.

Scottish Cyber Coordination Centre

Konni Deploys EndRAT Through Phishing, Uses KakaoTalk to Propagate Malware

The Hacker News - 17 March 2026 16:23

North Korean threat actors have been observed sending phishing to compromise targets and obtain access to a victim's KakaoTalk desktop application to distribute malicious payloads to certain contacts.

LeakNet ransomware uses ClickFix, Deno runtime in stealthy attacks

BleepingComputer - 17 March 2026 09:09

The LeakNet ransomware gang is now using the ClickFix technique for initial access into corporate environments and deploys a malware loader based on the open-source Deno runtime for JavaScript and TypeScript.

UK Related

UK Cyber Monitoring Centre Sets Its Sights on US Expansion One Year After Launch

Infosecurity Magazine - 17 March 2026 11:15

The US Cyber Monitoring Center should be operational in 2027. The UK-based nonprofit was established by a team of experts in February 2025 to assess the economic and financial impact of major cyber incidents occurring in the UK.