Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 March 2026

Vulnerabilities

Coruna iOS exploit framework linked to Triangulation attacks

BleepingComputer - 26 March 2026 10:10

The Coruna exploit kit is an evolution of the framework used in the Operation Triangulation espionage campaign, which in 2023 targeted iPhones via zero-click iMessage exploits.

Claude Extension Flaw Enabled Zero-Click XSS Prompt Injection via Any Website

The Hacker News - 26 March 2026 19:41

Cybersecurity researchers have disclosed a vulnerability in Anthropic's Claude Google Chrome Extension that could have been exploited to trigger malicious prompts simply by visiting a web page.

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-2026-33634 Aqua Security Trivy Embedded Malicious Code Vulnerability

BIND Updates Patch High-Severity Vulnerabilities

SecurityWeek - 26 March 2026 14:31

Specially crafted domains could be used to cause out-of-memory conditions, leading to memory leaks in the BIND resolvers.

Cisco Patches Multiple Vulnerabilities in IOS Software

SecurityWeek - 26 March 2026 13:32

The high- and medium-severity flaws could lead to denial-of-service, secure boot bypass, information disclosure, and privilege escalation.

Threat actors and malware

China-Linked Red Menshen Uses Stealthy BPFDoor Implants to Spy via Telecom Networks

The Hacker News - 27 March 2026 00:10

A long-term and ongoing campaign attributed to a China-nexus threat actor has embedded itself in telecom networks to conduct espionage against government networks.

Scottish Cyber Coordination Centre

Iran-Linked Pay2Key Ransomware Group Re-Emerges

Infosecurity Magazine - 26 March 2026 11:45

Halcyon and Beazley Security track the return of Iranian ransomware group Pay2Key