Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

5 March 2026

Vulnerabilities

Cisco warns of max severity Secure FMC flaws giving root access

BleepingComputer - 04 March 2026 15:12

Cisco has released security updates to patch two maximum-severity vulnerabilities in its Secure Firewall Management Center (FMC) software. [...]

U.S. CISA adds Qualcomm and Broadcom VMware Aria Operations flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 04 March 2026 09:56

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Qualcomm and Broadcom VMware Aria Operations flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Google Chromium CSS, Microsoft Windows, TeamT5 ThreatSonar Anti-Ransomware, and Zimbra flaws to its Known Exploited Vulnerabilities (KEV) catalog. Below are the flaws added to the catalog:

VMware Aria Operations Bug Exploited, Cloud Resources at Risk

darkreading - 04 March 2026 22:04

Exploitation of the command injection flaw in VMware Aria Operations could grant an attacker broad acess to victims' cloud environments.

High-severity Qualcomm bug hits Android devices in targeted attacks

Malwarebytes - 04 March 2026 13:33

Google has patched 129 Android vulnerabilities, including an actively exploited flaw in a widely used Qualcomm component.

Threat actors and malware

Spyware-grade Coruna iOS exploit kit now used in crypto theft attacks

BleepingComputer - 04 March 2026 15:06

A previously undocumented set of 23 iOS exploits named “Coruna” has been deployed by multiple threat actors in targeted espionage campaigns and financially motivated attacks. [...]

How a Brute Force Attack Unmasked a Ransomware Infrastructure Network

BleepingComputer - 04 March 2026 11:02

A routine RDP brute-force alert led to unusual credential hunting and a geo-distributed VPN-linked infrastructure. Huntress Labs explains how one compromised login unraveled a suspected ransomware-as-a-service ecosystem tied to initial access brokers. [...]

Europol-Led Operation Takes Down Tycoon 2FA Phishing-as-a-Service Linked to 64,000 Attacks

The Hacker News - 05 March 2026 13:21

Tycoon 2FA, one of the prominent phishing-as-a-service (PhaaS) toolkits that allowed cybercriminals to stage adversary-in-the-middle (AitM) credential harvesting attacks at scale, was dismantled by a coalition of law enforcement agencies and security companies.

149 Hacktivist DDoS Attacks Hit 110 Organizations in 16 Countries After Middle East Conflict

The Hacker News - 04 March 2026 23:51

Cybersecurity researchers have warned of a surge in retaliatory hacktivist activity following the U.S.-Israel coordinated military campaign against Iran, codenamed Epic Fury and Roaring Lion.

Iran Conflict and Cybersecurity: What to Expect in the Next 30 Days

Security Magazine - 04 March 2026 13:00

What to expect as the conflict between the United States and Iran unfolds.