Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 March 2026

Vulnerabilities

CISA flags VMware Aria Operations RCE flaw as exploited in attacks

BleepingComputer - 03 March 2026 19:40

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a VMware Aria Operations vulnerability tracked as CVE-2026-22719 to its Known Exploited Vulnerabilities catalog, flagging the flaw as exploited in attacks. [...]

Chrome security flaw enabled spying via Gemini Live assistant

Security Affairs - 03 March 2026 09:48

A Google Chrome vulnerability lets malicious extensions hijack Gemini Live to spy on users and steal sensitive files. Researchers at Palo Alto Networks found a Chrome vulnerability, tracked as CVE-2026-0628, that could let malicious extensions take control of the Gemini Live AI assistant.

Google Confirms CVE-2026-21385 in Qualcomm Android Component Exploited

The Hacker News - 03 March 2026 13:38

Google on Monday disclosed that a high-severity security flaw impacting an open-source Qualcomm component used in Android devices has been exploited in the wild.The vulnerability in question is CVE-2026-21385 (CVSS score: 7.8), a buffer over-read in the Graphics component.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2026-21385 Qualcomm Multiple Chipsets Memory Corruption Vulnerability, CVE-2026-22719 Broadcom VMware Aria Operations Command Injection Vulnerability.

Threat actors and malware

Microsoft: Hackers abuse OAuth error flows to spread malware

BleepingComputer - 03 March 2026 16:59

Hackers are abusing the legitimate OAuth redirection mechanism to bypass phishing protections in email and browsers to take users to malicious pages. [...]

Scottish Cyber Coordination Centre

Open-Source CyberStrikeAI Deployed in AI-Driven FortiGate Attacks Across 55 Countries

The Hacker News - 03 March 2026 20:59

The threat actor behind the recently disclosed artificial intelligence (AI)-assisted campaign targeting Fortinet FortiGate appliances leveraged an open-source, AI-native security testing platform called CyberStrikeAI to execute the attacks.

As War Continues, Pro-Iranian Actors Launch Barrage of Cyberattacks

darkreading - 03 March 2026 12:30

Iran and its supporters have taken to cyberspace to retaliate for US-Israeli military action, with an aim to cause economic and physical disruption.