Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 April 2026

Vulnerabilities

New Chrome Zero-Day CVE-2026-5281 Under Active Exploitation — Patch Released

The Hacker News - 01 April 2026 18:12

Google on Thursday released security updates for its Chrome web browser to address 21 vulnerabilities, including a zero-day flaw that it said has been exploited in the wild. The high-severity vulnerability, CVE-2026-5281 (CVSS score: N/A), concerns a use-after-free bug in Dawn, an open-source and cross-platform implementation of the WebGPU standard.

Hackers exploit TrueConf zero-day to push malicious software updates

BleepingComputer - 01 April 2026 18:35

Hackers have targeted TrueConf conference servers in attacks that exploit a zero-day vulnerability, allowing them to execute arbitrary files on all connected endpoints.

Threat actors and malware

New CrystalRAT malware adds RAT, stealer and prankware features

BleepingComputer - 01 April 2026 20:17

A new malware-as-a-service called CrystalRAT is being promoted on Telegram, offering remote access, data theft, keylogging, and clipboard hijacking capabilities.

New DeepLoad Malware Dropped in ClickFix Attacks

SecurityWeek - 01 April 2026 16:04

The malware steals credentials, installs a malicious browser extension, and can spread via USB drives.

'NoVoice' Android malware on Google Play infected 2.3 million devices

BleepingComputer - 01 April 2026 15:07

A new Android malware named NoVoice was found on Google Play, hidden in more than 50 apps that were downloaded at least 2.3 million times.

Apple expands iOS 18 updates to more iPhones to block DarkSword attacks

BleepingComputer - 01 April 2026 18:50

Apple has now made it possible for more iPhones still running iOS 18 to receive security updates that protect against the actively exploited DarkSword exploit kit.

Scottish Cyber Coordination Centre

UK incidents

UK manufacturers under cyber fire with 80% reporting attacks

The Register - 01 April 2026 09:30

Nearly 80 percent of British manufacturers say they've been hit by a cyber incident in the past year, as new research suggests disruption on the factory floor is no longer an exception but business as usual.