Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 March 2026

Vulnerabilities

ClawJacked flaw exposed OpenClaw users to data theft

Security Affairs - 02 March 2026 10:42

“ClawJacked” flaw let malicious sites hijack OpenClaw AI agents to steal data; patch released in version 2026.2.26. A high-severity vulnerability called ClawJacked in OpenClaw allowed malicious websites to brute-force and take control of local AI agent instances.

New Chrome Vulnerability Let Malicious Extensions Escalate Privileges via Gemini Panel

The Hacker News - 02 March 2026 23:38

Cybersecurity researchers have disclosed details of a now-patched security flaw in Google Chrome that could have permitted attackers to escalate privileges and gain access to local files on the system.The vulnerability, tracked as CVE-2026-0628 (CVSS score: 8.8), has been described as a case of insufficient policy enforcement in the WebView tag.

Bug in Google’s Gemini AI Panel Opens Door to Hijacking

darkreading - 02 March 2026 11:27

Attackers could have exploited the vulnerability to escalate privileges, violate user privacy while browsing, and access sensitive resources.

Threat actors and malware

Russia-linked APT28 exploited MSHTML zero-day CVE-2026-21513 before patch

Security Affairs - 02 March 2026 15:45

Russia-linked APT28 reportedly exploited MSHTML zero-day CVE-2026-21513 before Microsoft patched it, a high-severity bypass flaw. Akamai reports that Russia-linked APT28 may have exploited CVE-2026-21513 CVSS score of 8.8), a high-severity MSHTML vulnerability (CVSS 8.8), before Microsoft patched it in February 2026.

North Korean Hackers Target Developers Through npm Packages

Security Boulevard - 02 March 2026 18:00

Open-source ecosystems power modern software development. Millions of developers rely on public repositories to accelerate innovation and reduce development time. That trust, however, is increasingly being weaponized. New reporting from The Hacker News reveals that North Korean threat actors have published 26 malicious packages to the npm registry in an attempt to compromise developer environments

Scottish Cyber Coordination Centre

Iran's cyberwar has begun

The Register - 02 March 2026 21:52

'Expect elevated activity for the foreseeable future' Iranian hackers have launched spying expeditions, digital probes, and distributed denial of service (DDoS) attacks in the wake of the US and Israel launching missile strikes over the weekend, and security researchers urge organizations to expect more cyber intrusions as the war continues....

North Korean APT Targets Air-Gapped Systems in Recent Campaign

SecurityWeek - 02 March 2026 12:46

Using Windows shortcut files, the APT deployed a new implant, a loader, a propagation tool, and two backdoors.

Ransomware Payments Decline 8% as Attacks Surge 50%

Infosecurity Magazine - 02 March 2026 11:45

Chainalysis reveals a big surge in median ransomware payment size in 2025 despite overall drop in criminal revenue

UK related

UK warns of Iranian cyberattack risks amid Middle-East conflict

BleepingComputer - 02 March 2026 11:54

The United Kingdom's National Cyber Security Centre (NCSC) alerted British organizations to a heightened risk of Iranian cyberattacks amid the ongoing conflict in the Middle East. [...]