Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 February 2026

Vulnerabilities

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-2026-1731 BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability.

CISA flags critical Microsoft SCCM flaw as exploited in attacks

BleepingComputer - 13 February 2026 08:35

CISA ordered federal agencies on Thursday to secure their systems against a critical Microsoft Configuration Manager vulnerability patched in October 2024 and now exploited in attacks. [...]

Google: state-backed hackers exploit Gemini AI for cyber recon and attacks

Security Affairs - 13 February 2026 11:57

Google says nation-state actors used Gemini AI for reconnaissance and attack support in cyber operations. Google DeepMind and GTIG report a rise in model extraction or “distillation” attacks aimed at stealing AI intellectual property, which Google has detected and blocked. While APT groups have not breached frontier models, private firms and researchers have tried to [...]

Attackers finally get around to exploiting critical Microsoft bug from 2024

The Register - 13 February 2026 19:45

As if admins haven’t had enough to do this week Ignore patches at your own risk. According to Uncle Sam, a SQL injection flaw in Microsoft Configuration Manager patched in October 2024 is now being actively exploited, exposing unpatched businesses and government agencies to attack....

Google Patches First Actively Exploited Chrome Zero-Day of 2026

SecurityWeek - 16 February 2026 08:54

A Chrome 145 update fixes CVE-2026-2441, a vulnerability that can likely be exploited for arbitrary code execution.

Threat actors and malware

New ClickFix attack abuses nslookup to retrieve PowerShell payload via DNS

BleepingComputer - 15 February 2026 20:29

Threat actors are now abusing DNS queries as part of ClickFix social engineering attacks to deliver malware, making this the first known use of DNS as a channel in these campaigns. [...]

CTM360: Lumma Stealer and Ninja Browser malware campaign abusing Google Groups

BleepingComputer - 15 February 2026 12:30

CTM360 reports 4,000+ malicious Google Groups and 3,500+ Google-hosted URLs used to spread the Lumma Stealer infostealing malware and a trojanized “Ninja Browser.”

One threat actor responsible for 83% of recent Ivanti RCE attacks

BleepingComputer - 14 February 2026 12:02

Threat intelligence observations show that a single threat actor is responsible for most of the active exploitation of two critical vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), tracked as CVE-2026-1281 and CVE-2026-1340. [...]

Claude LLM artifacts abused to push Mac infostealers in ClickFix attack

BleepingComputer - 13 February 2026 16:21

Threat actors are abusing Claude artifacts and Google Ads in ClickFix campaigns that deliver infostealer malware to macOS users searching for specific queries. [...]

Malicious npm and PyPI packages linked to Lazarus APT fake recruiter campaign

Security Affairs - 15 February 2026 19:13

Researchers found malicious npm and PyPI packages tied to a fake recruitment campaign linked to North Korea’s Lazarus Group. ReversingLabs researcher uncovered new malicious packages on npm and PyPI connected to a fake job recruitment campaign attributed to the North Korea-linked Lazarus Group.

Google Links China, Iran, Russia, North Korea to Coordinated Defense Sector Cyber Operations

The Hacker News - 13 February 2026 22:53

Several state-sponsored actors, hacktivist entities, and criminal groups from China, Iran, North Korea, and Russia have trained their sights on the defense industrial base (DIB) sector, according to findings from Google Threat Intelligence Group (GTIG).

Nation-State Hackers Put Defense Industrial Base Under Siege

darkreading - 13 February 2026 18:07

Espionage groups from China, Russia and other nations burned at least two dozen zero-days in edge devices in attempts to infiltrate defense contractors’ networks.

AI and RaaS Alter Threat Landscape, New Ransomware Groups Grow by 30%

Security Boulevard - 16 February 2026 08:00

Scottish Cyber Coordination Centre

AI automation, RaaS, a significant bump in vulnerability disclosures, and a rise in new ransomware gangs are reshaping the threat landscape and forcing defenders to change strategies.