Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 February 2026

Vulnerabilities

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2019-19006 Sangoma FreePBX Improper Authentication Vulnerability

CVE-2021-39935 GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability

CVE-2025-40551 SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

CVE-2025-64328 Sangoma FreePBX OS Command Injection Vulnerability

Hackers abused React Native CLI flaw to deploy Rust malware before public disclosure

Security Affairs - 03 February 2026 16:41

Hackers exploit a critical React Native CLI flaw (CVE-2025-11953) to run remote commands and drop stealthy Rust malware, weeks before public disclosure.

Hackers Exploit Metro4Shell RCE Flaw in React Native CLI npm Package

The Hacker News - 03 February 2026 20:30

Threat actors have been observed exploiting a critical security flaw impacting the Metro Development Server in the popular “@react-native-community/cli” npm package.Cybersecurity company VulnCheck said it first observed exploitation of CVE-2025-11953 (aka Metro4Shell) on December 21, 2025.

Docker Fixes Critical Ask Gordon AI Flaw Allowing Code Execution via Image Metadata

The Hacker News - 03 February 2026 23:11

Cybersecurity researchers have disclosed details of a now-patched security flaw impacting Ask Gordon, an artificial intelligence (AI) assistant built into Docker Desktop and the Docker Command-Line Interface (CLI), that could be exploited to execute code and exfiltrate sensitive data.

Scottish Cyber Coordination Centre

APT28 Uses Microsoft Office CVE-2026-21509 in Espionage-Focused Malware Attacks

The Hacker News - 03 February 2026 15:42

The Russia-linked state-sponsored threat actor known as APT28 (aka UAC-0001) has been attributed to attacks exploiting a newly disclosed security flaw in Microsoft Office as part of a campaign codenamed Operation Neusploit.

Threat actors and malware

Notepad++ infrastructure hack likely tied to China-nexus APT Lotus Blossom

Security Affairs - 03 February 2026 10:35

Rapid7 researchers say the Notepad++ hosting breach is likely linked to the China-nexus Lotus Blossom APT group. Recently, the Notepad++ maintainer revealed that nation-state hackers compromised the hosting provider's infrastructure, redirecting update traffic to malicious servers.

GlassWorm Malware Returns to Shatter Developer Ecosystems

darkreading - 03 February 2026 21:55

The self-replicating malware has poisoned a fresh set of Open VSX software components, leaving potential downstream victims with infostealer infections.

New Password-Stealing Phishing Campaign Targets Corporate Dropbox Credentials

Infosecurity Magazine - 03 February 2026 11:55

Multi-stage attack begins with fake message relating to business requests and evades detection with link hidden in a PDF.