Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

3 February 2026

Vulnerabilities

Russian hackers exploit recently patched Microsoft Office bug in attacks

BleepingComputer - 02 February 2026 17:00

Ukraine's Computer Emergency Response Team (CERT) says that Russian hackers are exploiting CVE-2026-21509, a recently patched vulnerability in multiple versions of Microsoft Office. [...]

Nation-state hack exploited hosting infrastructure to hijack Notepad++ updates

Security Affairs - 02 February 2026 11:55

Notepad++ maintainer says nation-state attackers hijacked the app's update system by redirecting traffic at the hosting provider level. The Notepad++ maintainer revealed that nation-state hackers compromised the hosting provider's infrastructure, redirecting update traffic to malicious servers.

OpenClaw Bug Enables One-Click Remote Code Execution via Malicious Link

The Hacker News - 02 February 2026 22:58

A high-severity security flaw has been disclosed in OpenClaw (formerly referred to as Clawdbot and Moltbot) that could allow remote code execution (RCE) through a crafted malicious link.The issue, which is tracked as CVE-2026-25253 (CVSS score: 8.8), has been addressed in version 2026.1.29 released on January 30, 2026.

Threat actors and malware

New GlassWorm attack targets macOS via compromised OpenVSX extensions

BleepingComputer - 02 February 2026 18:04

A new GlassWorm malware attack through compromised OpenVSX extensions focuses on stealing passwords, crypto-wallet data, and developer credentials and configurations from macOS systems. [...]

Malicious MoltBot skills used to push password-stealing malware

BleepingComputer - 02 February 2026 15:11

More than 230 malicious packages for the personal AI assistant OpenClaw (formerly known as Moltbot and ClawdBot) have been published in less than a week on the tool's official registry and on GitHub. [...]

Notepad++ update feature hijacked by Chinese state hackers for months

BleepingComputer - 02 February 2026 10:53

Chinese state-sponsored threat actors were likely behind the hijacking of Notepad++ update traffic last year that lasted for almost half a year, the developer states in an official announcement today. [...]

Hackers exploit unsecured MongoDB instances to wipe data and demand ransom

Security Affairs - 02 February 2026 16:13

Over 1,400 exposed MongoDB servers have been hijacked and wiped by hackers, who left ransom notes after exploiting weak or missing access controls. Cybersecurity firm Flare reports that unsecured MongoDB databases remain easy targets, with 1,416 of 3,100 exposed servers compromised.

eScan Antivirus Update Servers Compromised to Deliver Multi-Stage Malware

The Hacker News - 02 February 2026 12:17

The update infrastructure for eScan antivirus, a security solution developed by Indian cybersecurity company MicroWorld Technologies, has been compromised by unknown attackers to deliver a persistent downloader to enterprise and consumer systems.

Attackers Harvest Dropbox Logins Via Fake PDF Lures

darkreading - 02 February 2026 23:21

A malware-free phishing campaign targets corporate inboxes and asks employees to view "request orders," ultimately leading to Dropbox credential theft.

Android RAT Uses Hugging Face to Host Malware

Infosecurity Magazine - 02 February 2026 11:30

Bitdefender has discovered a new Android malware campaign that uses Hugging Face

AI Coding Assistants Secretly Copying All Code to China

Schneier on Security - 02 February 2026 13:05

There’s a new report about two AI coding assistants, used by 1.5 million developers, that are surreptitiously sending a copy of everything they ingest to China.Maybe avoid using them.