Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

13 January 2026

Vulnerabilities

Max severity Ni8mare flaw impacts nearly 60,000 n8n instances

BleepingComputer - 12 January 2026 10:05

Nearly 60,000 n8n instances exposed online remain unpatched against a maximum-severity vulnerability dubbed “Ni8mare.” [...]

GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials

The Hacker News - 12 January 2026 17:18

A new wave of GoBruteforcer attacks has targeted databases of cryptocurrency and blockchain projects to co-opt them into a botnet that’s capable of brute-forcing user passwords for services such as FTP, MySQL, PostgreSQL, and phpMyAdmin on Linux servers.

Critical jsPDF Vulnerability Enables Arbitrary File Read in Node.js (CVE-2025-68428)

Security Boulevard - 12 January 2026 18:42

In January 2026, a critical security vulnerability was disclosed in jsPDF, a popular JavaScript library used to generate PDF documents. The issue, tracked as CVE-2025-68428, affects server-side Node.js deployments of jsPDF prior to version 4.0.0 and has been assigned a CVSS score of 9.2. The vulnerability is a path traversal issue that can be abused

Instagram Fixes Password Reset Vulnerability Amid User Data Leak

SecurityWeek - 12 January 2026 15:13

The social media platform confirmed that the issue allowed third parties to send password reset emails to Instagram users.

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-2025-8110 Gogs Path Traversal Vulnerability This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise.

Threat actors and malware

Target’s dev server offline after hackers claim to steal source code

BleepingComputer - 12 January 2026 13:52

Hackers are claiming to be selling internal source code belonging to Target Corporation, after publishing what appears to be a sample of stolen code repositories on a public software development platform.

GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials

The Hacker News - 12 January 2026 17:18

A new wave of GoBruteforcer attacks has targeted databases of cryptocurrency and blockchain projects to co-opt them into a botnet that's capable of brute-forcing user passwords for services such as FTP, MySQL, PostgreSQL, and phpMyAdmin on Linux servers.

LLMs in Attacker Crosshairs, Warns Threat Intel Firm

SecurityWeek - 12 January 2026 12:53

Threat actors are hunting for misconfigured proxy servers to gain access to APIs for various LLMs.