Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 January 2026

Vulnerabilities

CERT/CC Warns binary-parser Bug Allows Node.js Privilege-Level Code Execution

The Hacker News - 21 January 2026 12:34

A security vulnerability has been disclosed in the popular binary-parser npm library that, if successfully exploited, could result in the execution of arbitrary JavaScript. The vulnerability, tracked as CVE-2026-1245 (CVSS score: N/A), affects all versions of the module prior to version 2.3.0, which addresses the issue.

Critical TP-Link VIGI camera flaw allowed remote takeover of surveillance systems

Security Affairs - 20 January 2026 16:20

TP-Link fixed a high-severity flaw, tracked as CVE-2026-0629 (CVSS score 8.7), affecting over 32 VIGI C and VIGI InSight camera models.

Cloudflare Fixes ACME Validation Bug Allowing WAF Bypass to Origin Servers

The Hacker News - 20 January 2026 17:42

Cloudflare has addressed a security vulnerability impacting its Automatic Certificate Management Environment (ACME) validation logic that made it possible to bypass security controls and access origin servers.

Google Gemini Flaw Turns Calendar Invites Into Attack Vector

darkreading - 20 January 2026 16:52

The indirect prompt injection vulnerability allows an attacker to weaponize invites to circumvent Google's privacy controls and access private data.

Anthropic quietly fixed flaws in its Git MCP server that allowed for remote code execution

The Register - 20 January 2026 14:00

Prompt injection for the win Anthropic has fixed three bugs in its official Git MCP server that researchers say can be chained with other MCP tools to remotely execute malicious code or overwrite files via prompt injection.

Chainlit Vulnerabilities May Leak Sensitive Information

SecurityWeek - 20 January 2026 15:13

The two bugs, an arbitrary file read and an SSRF bug, can be exploited without user interaction to leak credentials, databases, and other data.

Scottish Cyber Coordination Centre

Threat actors and malware

PDFSIDER Malware – Exploitation of DLL Side-Loading for AV and EDR Evasion

Security Affairs - 20 January 2026 22:17

Resecurity has learned about PDFSIDER during an investigation of a network intrusion attempt that was successfully prevented by a Fortune 100 energy corporation.

Hackers Use LinkedIn Messages to Spread RAT Malware Through DLL Sideloading

The Hacker News - 20 January 2026 20:16

Cybersecurity researchers have uncovered a new phishing campaign that exploits social media private messages to propagate malicious payloads, likely with the intent to deploy a remote access trojan (RAT).

'CrashFix' Scam Crashes Browsers, Delivers Malware

darkreading - 20 January 2026 22:10

The attack consists of a NexShield malicious browser extension, a social engineering technique to crash the browser, and a Python-based RAT.

VoidLink cloud malware shows clear signs of being AI-generated

BleepingComputer - 20 January 2026 15:35

The recently discovered cloud-focused VoidLink malware framework is believed to have been developed by a single person with the help of an artificial intelligence model.

UK incidents

UK NCSC warns of Russia-linked hacktivists DDoS attacks

Security Affairs - 20 January 2026 09:21

The UK government warns that Russia-linked hacktivists are continuing DDoS attacks against critical infrastructure and local government systems.

UK launches landmark 'Report Fraud' service to tackle cybercrime and fraud

The Record from Recorded Future News - 20 January 2026 14:03

British authorities on Tuesday formally launched Report Fraud, a new national service aimed at overhauling how fraud and cybercrime victims contact police and how those incidents are subsequently investigated.