Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 January 2026

Vulnerabilities

Cisco fixes Unified Communications RCE zero day exploited in attacks

BleepingComputer - 21 January 2026 18:16

Cisco has fixed a critical Unified Communications and Webex Calling remote code execution vulnerability, tracked as CVE-2026-20045, that has been actively exploited as a zero-day in attacks.

Fortinet admins report patched FortiGate firewalls getting hacked

BleepingComputer - 21 January 2026 13:49

Fortinet customers are seeing attackers exploiting a patch bypass for a previously fixed critical FortiGate authentication vulnerability (CVE-2025-59718) to hack patched firewalls.

Zoom and GitLab Release Security Updates Fixing RCE, DoS, and 2FA Bypass Flaws

The Hacker News - 21 January 2026 22:12

Zoom and GitLab have released security updates to resolve a number of security vulnerabilities that could result in denial-of-service (DoS) and remote code execution. The most severe of the lot is a critical security flaw impacting Zoom Node Multimedia Routers (MMRs) that could permit a meeting participant to conduct remote code execution attacks.

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: 6.5), affects all versions of the module prior to version 2.3.0, which addresses the issue.

Zoom fixed critical Node Multimedia Routers flaw

Security Affairs - 21 January 2026 19:33

Cloud-based video conferencing and online collaboration platform Zoom released security updates to address multiple vulnerabilities, including command injection, tracked as CVE-2026-22844 (CVSS score of 9.9), in Zoom Node Multimedia Routers (MMRs) that could result in remote code execution.

Tesla hacked, 37 zero-days demoed at Pwn2Own Automotive 2026

BleepingComputer - 21 January 2026 08:16

Security researchers have hacked the Tesla Infotainment System and earned $516,500 after exploiting 37 zero-days on the first day of the Pwn2Own Automotive 2026 competition.

Threat actors and malware

LastPass Users Targeted With Backup-Themed Phishing Emails

SecurityWeek - 21 January 2026 14:47

Threat actors may have wanted to take advantage of the holiday weekend in the United States to increase their chances of success.

New Android malware uses AI to click on hidden browser ads

BleepingComputer - 21 January 2026 18:07

A new family of Android click-fraud trojans leverages TensorFlow machine learning models to automatically detect and interact with specific advertisement elements.