Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 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-2008-0015 Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability

CVE-2020-7796 Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability

CVE-2024-7694 TeamT5 ThreatSonar Anti-Ransomware Unrestricted Upload of File with Dangerous Type Vulnerability

CVE-2026-2441 Google Chromium CSS Use-After-Free Vulnerability

Dell RecoverPoint Zero-Day Exploited by Chinese Cyberespionage Group

SecurityWeek - 18 February 2026 08:09

GTIG and Mandiant said the zero-day tracked as CVE-2026-22769 has been exploited by UNC6201 since at least 2024.

Update Chrome now: Zero-day bug allows code execution via malicious webpages

Malwarebytes - 17 February 2026 13:33

Google has released an emergency update to patch an actively exploited zero-day—the first Chrome zero-day of the year.

Flaws in popular VSCode extensions expose developers to attacks

BleepingComputer - 17 February 2026 17:27

Vulnerabilities with high to critical severity ratings affecting popular Visual Studio Code (VSCode) extensions collectively downloaded more than 128 million times could be exploited to steal local files and execute code remotely.

Threat actors and malware

SmartLoader Attack Uses Trojanized Oura MCP Server to Deploy StealC Infostealer

The Hacker News - 17 February 2026 19:12

Cybersecurity researchers have disclosed details of a new SmartLoader campaign that involves distributing a trojanized version of a Model Context Protocol (MCP) server associated with Oura Health to deliver an information stealer known as StealC.

Scottish Cyber Coordination Centre

ClickFix Attacks Abuses DNS Lookup Command to Deliver ModeloRAT

darkreading - 17 February 2026 22:01

ClickFix campaigns have adapted to the latest defenses with a new technique to trick users into infecting their own machines with malware.

Researchers Show Copilot and Grok Can Be Abused as Malware C2 Proxies

The Hacker News - 18 February 2026 00:38

Cybersecurity researchers have disclosed that artificial intelligence (AI) assistants that support web browsing or URL fetching capabilities can be turned into stealthy command-and-control (C2) relays, a technique that could allow attackers to blend into legitimate enterprise communications and evade detection.

API Threats Grow in Scale as AI Expands the Blast Radius

SecurityWeek - 17 February 2026 15:00

New research shows attackers increasingly abusing APIs at machine speed as AI-driven systems widen exposure and amplify impact.

UK Related

UK.gov launches cyber ‘lockdown’ campaign as 80% of orgs still leave door open

The Register - 17 February 2026 12:30

Digital burglaries remain routine, and data shows most corps still don’t stick to basic infosec standards Britain is telling businesses to “lock the door” on cybercrims as new government data suggests most still haven’t even found the latch.