



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

10 February 2025

Vulnerabilities

[U.S. CISA adds Trimble Cityworks flaw to its Known Exploited Vulnerabilities catalog](#)

Security Affairs - 07 February 2025 22:54

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Trimble Cityworks vulnerability, tracked as CVE-2025-0994, to its Known Exploited Vulnerabilities (KEV) catalog. Trimble Cityworks is a GIS-centric asset management and permitting software designed for local governments, utilities, and public works organizations.

[Hackers Exploiting SimpleHelp RMM Flaws for Persistent Access and Ransomware](#)

The Hacker News - 07 February 2025 11:49

Threat actors have been observed exploiting recently disclosed security flaws in SimpleHelp's Remote Monitoring and Management (RMM) software as a precursor for what appears to be a ransomware attack.

Threat actors and malware

[Massive brute force attack uses 2.8 million IPs to target VPN devices](#)

BleepingComputer - 08 February 2025 11:15

A large-scale brute force password attack using almost 2.8 million IP addresses is underway, attempting to guess the credentials for a wide range of networking devices, including those from Palo Alto Networks, Ivanti, and SonicWall.

[Cloudflare outage caused by botched blocking of phishing URL](#)

BleepingComputer - 07 February 2025 11:44

An attempt to block a phishing URL in Cloudflare's R2 object storage platform backfired yesterday, triggering a widespread outage that brought down multiple services for nearly an hour.

[DeepSeek-impersonating malware is stealing data, research finds](#)

Security Magazine - 07 February 2025 10:00

The emergence of DeepSeek has led to malicious actors attempting to exploit its prominence.



Scottish
Cyber
Coordination
Centre

UK Specific

[UK Engineering Giant IMI Hit by Cyberattack](#)

SecurityWeek - 07 February 2025 13:06

UK engineering firm IMI says it suffered a cyberattack that resulted in unauthorized access to some of its systems.

[UK Home Office silent on alleged Apple backdoor order](#)

The Register - 07 February 2025 18:03

The UK's Home Office refuses to either confirm or deny reports that it recently ordered Apple to create a backdoor allowing the government to access any user's cloud data.