



Daily Threat Bulletin

30 December 2025

Vulnerabilities

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CVE-2025-14847 MongoDB and MongoDB Server

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-14847 MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CVE-2025-14733 WatchGuard Firebox

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-14733 WatchGuard Firebox Out-of-Bounds Write

[CISA Adds Three Known Exploited Vulnerabilities to Catalog](#)

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-20393 Cisco Multiple Products Improper Input Validation Vulnerability CVE-2025-40602 SonicWall SMA1000 Missing Authorization Vulnerability CVE-2025-59374 ASUS Live Update Embedded Malicious Code

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CVE-2025-59718 Fortinet

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-59718 Fortinet Multiple Products Improper Verification of Cryptographic Signature

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CVE-2025-14174 Google Chromium

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-14174 Google Chromium Out-of-Bounds Memory Access

Threat actors and malware

[Romanian energy provider hit by Gentlemen ransomware attack](#)



Scottish
Cyber
Coordination
Centre

A ransomware attack hit Oltenia Energy Complex (Complexul Energetic Oltenia), Romania's largest coal-based energy producer, on the second day of Christmas, taking down its IT infrastructure.

[CISA and Partners Release Update to Malware Analysis Report BRICKSTORM Backdoor](#)

CISA Advisories -

Today, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and Canadian Centre for Cyber Security released an update to the Malware Analysis Report BRICKSTORM Backdoor with indicators of compromise (IOCs) and detection signatures for additional BRICKSTORM samples.

UK related

[Evasive Panda cyberespionage campaign uses DNS poisoning to install MgBot backdoor](#)

China-linked APT Evasive Panda used DNS poisoning to deliver the MgBot backdoor in targeted cyber-espionage attacks in Türkiye, China, and India. Kaspersky researchers spotted the China-linked APT group Evasive Panda (aka Daggerfly, Bronze Highland, and StormBamboo) running a targeted cyber-espionage campaign using DNS poisoning to deliver the MgBot backdoor against victims