



Daily Threat Bulletin

29 December 2025

Vulnerabilities

[Exploited MongoBleed flaw leaks MongoDB secrets, 87K servers exposed](#)

BleepingComputer - 28 December 2025 16:38

A severe vulnerability affecting multiple MongoDB versions, dubbed MongoBleed (CVE-2025-14847), is being actively exploited in the wild, with over 80,000 potentially vulnerable servers exposed on the public web.

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

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2023-52163 Digiever DS-2105 Pro Missing Authorization Vulnerability This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks.

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

CISA Advisories -

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 Vulnerability. This type of vulnerability is a frequent attack vector for malicious cyber actors.

Threat actors and malware

[Hacker claims to leak WIRED database with 2.3 million records](#)

BleepingComputer - 28 December 2025 13:57

A hacker claims to have breached Condé Nast and leaked an alleged WIRED database containing more than 2.3 million subscriber records, while also warning that they plan to release up to 40 million additional records for other Condé Nast properties.



Scottish
Cyber
Coordination
Centre

UK related

Cybersecurity Performance Goals 2.0 for Critical Infrastructure

CISA Advisories -

Today, CISA released updated Cross-Sector Cybersecurity Performance Goals (CPG 2.0) with measurable actions for critical infrastructure owners and operators to achieve a foundational level of cybersecurity. This update incorporates lessons learned, aligns with the most recent National Institute of Standards and Technology Cybersecurity Framework revisions, and addresses the most common and impactful threats facing critical infrastructure today.