

CISA Flags Two Actively Exploited Zammad Vulnerabilities for Priority Remediation



CISA has added two actively exploited vulnerabilities in Zammad software to its Known Exploited Vulnerabilities Catalog, urging organizations to prioritize remediation of session fixation and privilege management flaws.

- Two Zammad vulnerabilities (CVE-2026-102489 and CVE-2026-102490) added to CISA's KEV Catalog due to active exploitation
- Flaws involve session fixation and improper privilege management, common attack vectors for threat actors
- CISA urges all organizations, not only US federal agencies, to adopt risk-based vulnerability management
- Vulnerabilities on publicly exposed assets that grant total control post-exploitation require rapid

remediation

- Organizations should verify whether systems were compromised before applying patches

The US Cybersecurity and Infrastructure Security Agency has added two vulnerabilities affecting Zammad software to its Known Exploited Vulnerabilities Catalog following evidence of active exploitation in the wild. The additions underscore ongoing risks from common attack patterns targeting session management and access controls.

Vulnerabilities and Risk Profile

The two flaws are **CVE-2026-102489**, a session fixation vulnerability, and **CVE-2026-102490**, an improper privilege management vulnerability. Both affect Zammad GmbH's Zammad platform. CISA notes that these vulnerability types represent frequent attack vectors exploited by malicious actors and pose significant risks to enterprise environments, particularly when present on publicly exposed systems.

Under the agency's Binding Operational Directive 26-04, US federal agencies must prioritize rapid remediation of high-risk vulnerabilities—specifically those on publicly exposed assets that grant total control of the asset following successful exploitation. The directive also establishes expectations for agencies to determine whether threat actors compromised systems before patches were applied.

Guidance for All Organizations

While the directive applies only to US federal civilian agencies, CISA encourages all organizations worldwide to adopt **risk-based vulnerability management** practices and prioritize remediation of vulnerabilities listed in the KEV Catalog. The agency continues to update the catalog based on evidence of active exploitation and clear mitigation guidance.

Organizations aware of exploited vulnerabilities not yet listed may submit them through CISA's KEV Nomination Form, provided they have a CVE identifier, evidence of exploitation, and available mitigation steps.

What to do now

1. Identify all instances of Zammad software in your environment, particularly on publicly exposed systems
2. Apply vendor patches for CVE-2026-102489 and CVE-2026-102490 immediately on internet-facing Zammad deployments
3. Review authentication logs and session management records for signs of compromise before patch application
4. Conduct privilege escalation testing on patched systems to verify remediation effectiveness
5. Update vulnerability management procedures to prioritize KEV Catalog entries in line with NCA ECC and

SAMA CSF requirements

6. Document remediation timelines and verification steps for audit and compliance purposes