

Session Fixation Vulnerability in Zammad Enables Remote Code Execution



A session fixation vulnerability in Zammad GmbH Zammad can lead to remote code execution as the zammad user and may be chained with another vulnerability.

- Zammad GmbH Zammad contains a session fixation vulnerability tracked as CVE-2026-102489
- The vulnerability can lead to remote code execution with zammad user privileges
- The flaw can be chained with CVE-2026-102490 for potentially greater impact
- Vendor mitigations should be applied immediately or the product discontinued if patches are unavailable
- Organizations must evaluate internet exposure of affected assets and prioritize patching

Vulnerability Overview

Zammad GmbH Zammad, a web-based customer support and ticketing system, contains a **session fixation vulnerability** designated CVE-2026-102489. This security flaw allows attackers to potentially execute arbitrary code remotely with the privileges of the zammad user account. The vulnerability becomes particularly concerning when combined with CVE-2026-102490, enabling attackers to chain exploits for more severe compromise.

Session fixation attacks occur when an attacker can force a user's session identifier to a known value, allowing the attacker to hijack authenticated sessions. In this case, successful exploitation grants code execution capabilities, representing a significant risk to the confidentiality, integrity and availability of affected systems.

Risk Context for Saudi Institutions

Organizations using Zammad for customer service operations, IT service management or internal ticketing should treat this vulnerability as requiring immediate attention. The potential for remote code execution means attackers could gain unauthorized access to sensitive customer data, support tickets containing confidential information, or use compromised systems as pivot points for broader network intrusion.

Regulated entities in the Kingdom must evaluate whether Zammad instances are exposed to the internet and assess the sensitivity of data processed through these systems. The ability to chain this vulnerability with CVE-2026-102490 amplifies the urgency of remediation efforts.

Recommended Response

Organizations should immediately consult Zammad GmbH vendor guidance for available security updates and apply patches without delay. If mitigations are not available from the vendor, institutions should consider discontinuing use of the product until patches are released. Asset owners must conduct forensic triage if compromise is suspected and document all remediation activities for compliance purposes.

What to do now

1. Identify all Zammad instances deployed within your organization and document their internet exposure status
2. Consult Zammad GmbH vendor security advisories immediately for available patches and mitigation guidance
3. Apply vendor-provided security updates to all affected Zammad installations as a priority remediation activity
4. If patches are unavailable, evaluate discontinuing use of Zammad until vendor mitigations are released
5. Conduct forensic triage on Zammad systems if unauthorized access or anomalous activity is suspected
6. Review access logs and session management records for indicators of session fixation or exploitation

attempts