Take care: Local Privilege Escalation (CVE-2026-102490) is reported as being actively exploited

security

JuliaDenise 2 October 1, 2026, 12:16pm

Zammad statement on vulnerability reports in DIVD case DIVD-2026-00015

Zammad is aware of public reports about two vulnerabilities in Zammad. The reports are published in case DIVD-2026-00015 by the Dutch Institute for Vulnerability Disclosure (DIVD). The case has also been covered by media and third-party security sites. This statement gives our view on both reports.

CVE-2026-102489 – current Zammad versions are not affected

We first received a report about this issue in August 2026 and analysed it then. Exploitation is only possible on Zammad 6.5 and older, because of the runtime environment those versions use. These versions reached end of support some time ago. Under our security policy, we provide security fixes only for the current stable release.

Zammad 7.0 and later are not affected. DIVD's own case page also says that the issue cannot be exploited in practice on these versions. We have still hardened the affected code. The change is included in Zammad 7.2.0.

CVE-2026-102490 – no details received

The DIVD case page lists a second vulnerability, a local privilege escalation, and claims that it affects nearly every Zammad version ever released. Third-party sites describe it as being actively exploited. Up to today, DIVD has not given us any technical details about this vulnerability. We cannot verify a claim we have not been shown. This means we cannot confirm the vulnerability, its scope or the affected versions at this time.

We have formally asked DIVD to send us all available information. As soon as we receive it, we will work on it with the highest priority and publish verified results.

Our view on how this case was disclosed

Coordinated disclosure gives a vendor the details and a reasonable amount of time to fix an issue before it becomes public. That protects users. DIVD's own timeline shows a report to us on 24 September 2026, followed by public scanning and disclosure on 26 September 2026. A CVE identifier was published for a vulnerability we had not been told about, and its exploitation is now being discussed in public. This leaves Zammad administrators worried, and it leaves them without the information they need to act. We do not consider this a responsible way to handle vulnerabilities.

What we recommend to administrators

- Update to Zammad 7.2.0, the current stable release.
- If you still run Zammad 6.5 or older, update now. These versions no longer receive security fixes.
- Follow our security advisories at **Security Advisories · zammad/zammad · GitHub** for updates on CVE-2026-102490.

Contact for security researchers

Security researchers can report vulnerabilities at any time to **security@zammad.com**. Our public PGP key is available for encrypted messages. We are always willing to work with researchers who follow coordinated disclosure.

8 Likes

---

show post in topic