contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Zammad GmbH Zammad exploited

CVE-2026-102490 · on CISA's exploited list since 2 October 2026

Analysis Report

If you run Zammad from DEB or RPM packages, update to 7.2.2 now and limit who can log in to the server. Source or container installs can stop reading: the record says they are not affected.

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 9.4**	STATUS	On CISA's exploited list; due 5 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/zammad-gmbh-zammad-cve-2026-102490

The bottom line

> *If you run Zammad from DEB or RPM packages, update to 7.2.2 now and limit who can log in to the server. Source or container installs can stop reading: the record says they are not affected.*

At a glance

Fact	Detail
Product	Zammad GmbH Zammad (CVE-2026-102490)
Severity	Critical: 9.4 (CVSS 4.0)
CISA	On its exploited list since 2 October 2026. Deadline for US federal agencies: 5 October 2026.
Chance of exploitation (EPSS)	0.11, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	7.2.2 is the first unaffected version, per the record. The vendor's release list dates 7.2.2 to 8 October 2026 and says it covers a DEB/RPM-only flaw.
Who looks first	Anyone running Zammad installed from DEB or RPM packages (packager.io) on their own server, especially where several people or other applications can log in to that host.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Zammad on a server you or your provider manage?	Nothing to do for this CVE.	Check how it was installed (next question).
Was it installed from DEB or RPM packages, not from source or the official container image?	The record says source and container installs were not affected. Nothing to do.	Check the version (next question).
Is the installed version older than 7.2.2?	You are on the first unaffected version or later. Confirm it in writing.	Update to 7.2.2 and limit server access.

Can anyone besides trusted administrators log in to that server or run code on it?	The vendor says an attacker needs access to the server first, so exposure is lower. Still update.	Treat as urgent: remove that access and update.

What it is

Someone who already has write access as the zammad service account on the host can become root. The record says services started as root and ran files that the zammad account could write, then switched to that account.

Why it matters

The record gives a score of 9.4 even though the attacker needs a foothold first. The vendor's advisory says it cannot be exploited remotely on its own. Our reading is that it matters as a second step: any small break-in on the host, such as through another application, could become full control of the machine and the helpdesk data on it. The record says it took seconds, with no administrator action.

What the vendor's advisory says

We read three pages on zammad.com and community.zammad.org. In short:

- The vendor's advisory of 5 October 2026 calls this a local privilege escalation that needs prior access to the underlying server.
- It says the issue is related to a confirmed vulnerability in packager.io and that the team was working on a solution when it was written.
- It advises restricting access to the underlying Zammad server to trusted administrators only.
- It tells anyone on Zammad 6.5 or older to update immediately, because those versions no longer receive security updates.
- CISA says this can be chained with CVE-2026-102489. The vendor says that one is only exploitable on Zammad 6.5 and earlier.

Things people will get wrong

- "It is local only, so it can wait." CISA lists it as exploited, and the record says a foothold as the zammad account was enough. Any other flaw that gives that foothold makes this one reachable.
- "Every Zammad install is affected." The record says only DEB and RPM package installs were affected. Source and official container installs were not.
- "The vendor has not confirmed it, so there is nothing to apply." The vendor's earlier statement said so, but its 5 October advisory confirms it. The record lists 7.2.2 as the first unaffected

version.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find how Zammad is installed and which version

- Ask whoever runs the server whether Zammad came from DEB or RPM packages, source, or a container.
- Record the exact version. Anything below 7.2.2 on a package install is affected, per the record.

```
dpkg -l zammad
rpm -q zammad
```

Step 2: Reduce who can reach the server

- Limit server logins and shell access to trusted administrators, as the vendor advises.
- Remove accounts and remote-access routes that are not needed until the update is done.

Step 3: Update to 7.2.2 or later

- Install 7.2.2 or later from the package repository you already use, in a maintenance window.
- If you are on 6.5 or older, the vendor says to update now. Whether its 6.5.5 release covers this flaw is not stated.

Step 4: Check the result and look for signs of misuse

- Confirm the installed version is 7.2.2 or later.
- If the server was reachable by others before the update, check for files the zammad account could write that root-run services use, and for unexpected service restarts.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to check our exposure to CVE-2026-102490 in Zammad, a privilege escalation that affects installs from DEB or RPM packages. Please tell us whether we run Zammad, how it was installed, and which version. The record lists 7.2.2 as the first unaffected version. Please update anything older and restrict server access to trusted administrators until then. CISA lists this CVE as exploited, so please treat it as urgent. Please confirm in writing the installed version and that the fix is applied, by the end of this week.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Files owned by the zammad account in locations that root-run Zammad services execute from, especially any added or changed recently.
- Zammad services restarting or stopping unexpectedly, since the description says automatic restarts made the escalation quick.
- New root-level processes, accounts or scheduled tasks on the host that nobody on your team created.

The weakness behind it

CISA's entry classes this as CWE-269 (Improper Privilege Management).

The sources, in their words

CISA's catalogue entry:

> *Zammad GmbH Zammad contains an improper privilege management vulnerability that can allow the local zammad user to escalate privileges to root. This vulnerability can be chained with CVE-2026-102489.*

The CVE record, published by DIVD on 30 September 2026:

> *Zammad packages built with packager.io (DEB and RPM) could have allowed a local attacker who already had file system write privileges as the unprivileged zammad service account to escalate to full root privileges on the host. Service processes began running as root and executed files that were owned and writable by the zammad account before dropping their identity to that account. An attacker holding that foothold could have escalated within seconds, because the affected services were restarted automatically whenever they stopped; no administrator interaction was required. Only installations from the DEB and RPM packages were affected — installations from source or the official container …*

Versions of Zammad GmbH Zammad the record lists as affected:

- 1.5.0 up to, but not including, 7.2.2

It lists these as unaffected:

- 7.2.2

The affected ranges end before 7.2.2. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Whether Zammad 6.5.5, released on 15 October 2026, fixes this flaw. The sources do not link them.
- Which logs or files would show that the flaw was used. The sources give no indicators.
- How the attacker first gets the zammad-account foothold. The sources do not describe it.
- Whether any workaround exists besides restricting server access. The advisory names none.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-102490: score 9.4, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A/AU:Y/V:C` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	Passive	A person must be present but does nothing unusual.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
30 September 2026	CVE record published by DIVD.
2 October 2026	CISA added it to its list of exploited vulnerabilities.
5 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
A packaged Zammad below 7.2.2 on a server where other people or applications can log in	High	Now
A packaged Zammad below 7.2.2 where only trusted administrators have server access	High	Now; the fix is available and CISA lists it as exploited
Zammad 6.5 or older, packaged or not	High	Now; the vendor says these get no routine security updates
Zammad installed from source or the official container image	None	None for this CVE
Packaged Zammad already on 7.2.2 or later	Low	Confirm the version at the next check

Appendix 4. Definition of done

- Every Zammad GmbH Zammad you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-102490: https://www.cve.org/CVERecord?id=CVE-2026-102490
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: zammad.com/en/advisories/cve-2026-102489-cve-2026-102490: https://zammad.com/en/advisories/cve-2026-102489-cve-2026-102490
- Advisory or release notes read: zammad.com/en/product/releases/: https://zammad.com/en/product/releases/
- Advisory or release notes read: community.zammad.org/t/take-care-local-privilege-escalation-cve-2026: https://community.zammad.org/t/take-care-local-privilege-escalation-cve-2026-102490-is-reported-as-being-actively-exploited/21297/2
- Reference in the CVE record: csirt.divd.nl: https://csirt.divd.nl/DIVD-2026-00015
- Reference in the CVE record: csirt.divd.nl: https://csirt.divd.nl/CVE-2026-102490
- Reference in the CVE record: github.com: https://github.com/zammad/zammad/security/advisories/GHSA-p97w-927q-8vxq