contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Zammad GmbH Zammad exploited

CVE-2026-102489 · on CISA's exploited list since 2 October 2026

Analysis Report

If you run Zammad 6.5 or earlier, act now: CISA's date has already passed. Move to a supported release. If you run 7.0 or later, the vendor says this flaw cannot be exploited there, so you can stop …

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-2026-102489

The bottom line

> *If you run Zammad 6.5 or earlier, act now: CISA's date has already passed. Move to a supported release. If you run 7.0 or later, the vendor says this flaw cannot be exploited there, so you can stop reading.*

At a glance

Fact	Detail
Product	Zammad GmbH Zammad (CVE-2026-102489)
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)	0.22, 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	No fix for 6.5 or earlier is named for this CVE. The vendor says 7.0 and later are not affected in practice, with a hardening change in 7.2.0 (advisory, 5 October 2026).
Who looks first	Anyone self-hosting Zammad 6.3 to 6.5.x, especially if the helpdesk is reachable from the internet. The vendor says 7.0 and later are not affected in practice.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Zammad yourselves (not the vendor's hosted service)?	Nothing to do for this CVE.	Check the version (next question).
Is your Zammad version 6.5 or earlier?	The vendor says 7.0 and later are not exploitable. Plan an update to 7.2.0 or later.	Treat it as exposed. Go to the next question.
Can anyone outside your organisation reach the Zammad login page?	Lower exposure, but still plan the update from 6.5 or earlier.	Restrict access now, then update.

Has anyone untrusted had access to the Zammad server itself?	Continue with the update.	Treat the server as possibly compromised and ask your provider to review it.

What it is

An attacker can take over a login session (session fixation, CWE-384) and use that to run code on the Zammad server as the zammad user. CISA says it can be chained with CVE-2026-102490, a local privilege escalation.

Why it matters

Our reading: the record gives a score of 9.4 and CISA says the flaw can be chained with CVE-2026-102490. A code-execution foothold paired with a privilege escalation could give an attacker the whole server, and a helpdesk holds customer messages. The vendor says 6.5 and earlier no longer receive routine security updates, so the usual route of waiting for a patch does not apply.

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 says exploitation is only possible on Zammad 6.5 and earlier, because of the runtime environment those versions use.
- The vendor says these versions are out of support and receive no security updates, and says to update immediately if you still run them.
- The vendor says it changed the affected code as extra hardening, included in Zammad 7.2.0.
- The vendor's release list shows Zammad 6.5.5 on 15 October 2026, an exceptional emergency fix for the unsupported 6.5 series. It does not say which flaw this addresses.
- For CVE-2026-102490, the vendor says it is a local privilege escalation that needs prior access to the server, and advises limiting server access to trusted administrators.

Things people will get wrong

- "Every Zammad install is affected." The vendor says 7.0 and later are not affected in practice. The record also says the bug is not exploitable on 7.0.0 to 7.1.2.
- "It is only a local flaw, so it can wait." The record describes remote code execution. The local escalation is the separate CVE-2026-102490, which CISA says it can be chained with.
- "The old 6.5 series will get a normal fix." The vendor says 6.5 and earlier are out of support. It lists 6.5.5 as an exceptional emergency release and does not link it to this CVE.

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 the versions you run

- Find every Zammad install, including test servers and old containers.
- Note whether each is 6.5 or earlier, 7.0 and later, or hosted by the vendor.

```
dpkg -l zammad
rpm -q zammad
docker ps --format '{{.Image}}'
```

Step 2: Reduce exposure

- Limit who can reach the login page and the underlying server, using a VPN or an allow-list.
- The vendor advises restricting server access to trusted administrators.

Step 3: Update to a supported release

- Update to Zammad 7.2.0 or later, the version the vendor recommends. Do not stay on 6.5 or earlier.
- Back up before updating.

Step 4: Check for signs of misuse

- If an old version was exposed, ask your provider to review the server for unexpected logins, new admin users and unfamiliar processes.
- Ask for written confirmation of the version afterwards.

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. CISA lists CVE-2026-102489 in Zammad as exploited. Could you tell us whether we run Zammad, where, and which version? The vendor says 6.5 and earlier are affected and out of support, and that 7.0 and later are not affected in practice. It recommends 7.2.0. If we run 6.5 or earlier, please restrict access to the server now and plan an update. Please send us written confirmation of the version and the fix by an agreed date, and tell us whether the server needs a compromise check. Thank you.*

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:

- Unexpected logins or sessions for admin accounts on a Zammad 6.5 or earlier system.
- Unfamiliar processes or files owned by the zammad user.
- New admin users, changed settings or unexpected outbound connections from the server.

The weakness behind it

CISA's entry classes this as CWE-384 (Session Fixation).

The sources, in their words

CISA's catalogue entry:

> *Zammad GmbH Zammad contains a session fixation vulnerability that can lead to remote code execution as the zammad user. This vulnerability can be chained with CVE-2026-102490.*

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

> *Zammad versions 6.3.0 to 6.5.4 are vulnerable a session hijack vulnerability that leads to remote code execution as the zammad user. The bug is also present in version 7.0.0 to version 7.1.2, but not exploitable due to changes in the underlying framework.*

Versions of Zammad GmbH Zammad the record lists as affected:

- 6.3.0 up to, but not including, 6.5.4

The affected ranges end before 6.5.4. 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

- Which exact version first fixes this CVE on the 6.5 line: the sources do not link 6.5.5 to it.
- Whether 6.5.4 is affected: the record's range excludes it, but its description includes it.
- Which flaw Zammad 7.2.2, the packager.io package fix, addresses; the sources do not link it to this CVE.
- How attackers are using the flaw in practice: the sources give no detail.
- 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-2026-102489: 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
Zammad 6.5 or earlier, reachable from the internet	High	Now; CISA's window has passed
Zammad 6.5 or earlier, reachable only on an internal network	High	This week
Zammad 7.0 to 7.1.x	Low	Next patch cycle
Zammad 7.2.0 or later	None	None for this CVE
Vendor-hosted Zammad, nothing self-run	None	None for this CVE

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-2026-102489: https://www.cve.org/CVERecord?id=CVE-2026-102489
- 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: 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
- Advisory or release notes read: zammad.com/en/product/releases/: https://zammad.com/en/product/releases/
- 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-2026-102489