contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

AhsayCBS exploited

CVE-2026-105133 · on CISA's exploited list since 14 October 2026

Analysis Report

If you run AhsayCBS, act now: CISA's deadline of 17 October 2026 has passed. First find your version. If it is 9.15.2.69, 10.3.4.44 or earlier, ask your provider for the hotfix. If you do not run ...

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 2.0 7.5**	STATUS	On CISA's exploited list; due 17 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/ahsaycbs-cve-2026-105133

The bottom line

> *If you run AhsayCBS, act now: CISA's deadline of 17 October 2026 has passed. First find your version. If it is 9.15.2.69, 10.3.4.44 or earlier, ask your provider for the hotfix. If you do not run AhsayCBS, you can stop reading.*

At a glance

Fact	Detail
Product	AhsayCBS (CVE-2026-105133)
Severity	High: 7.5 (CVSS 2.0)
CISA	On its exploited list since 14 October 2026. Deadline for US federal agencies: 17 October 2026.
Chance of exploitation (EPSS)	0.79, 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	Hotfix 9.15.2.70 (v7, v8, v9) and 10.3.4.45 (v10), per the vendor's advisory of 12 October 2026. A partner portal login is needed. Reboot afterwards.
Who looks first	Anyone who runs AhsayCBS, the backup server software, on version 9.15.2.69, 10.3.4.44 or earlier, and especially IT providers who host it for customers.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run AhsayCBS, or does your IT provider run it for you?	Nothing to do for this CVE.	Find the version (next question).
Is the version 9.15.2.69, 10.3.4.44 or earlier?	If it is 9.15.2.70 or 10.3.4.45 or later, get written confirmation of the fix.	You are in the affected range. Ask for the hotfix.
Can the AhsayCBS web or API port be reached from the internet?	Exposure is lower, but still patch. The flaw is a remote authentication bypass.	Restrict access now and patch as the first job.

Did you apply the earlier patches 9.15.2.59 or 10.3.4.0 and stop there?	Check you are on the hotfix versions anyway.	The vendor says those patches did not fully fix this. Apply the hotfix.

What it is

A remote attacker can get past the login by manipulating the random parameter in the API's checkSysPwd function. The record says no valid credentials are needed and the exploit is public. CISA says it can be chained with CVE-2026-105134.

Why it matters

Our reading is that a login bypass on backup software is valuable to an attacker because the server holds copies of customer data and the means to manage them. The record scores it 7.5 on the older CVSS 2.0 scale, which understates how useful it is when chained with CVE-2026-105134, as CISA says. The vendor says its first patches were incomplete, so having patched earlier is not enough.

What the vendor's advisory says

We read one page on www.ahsay.com. In short:

- The vendor's advisory of 12 October 2026 covers CVE-2026-105133 and CVE-2026-105134 together.
- The vendor says its earlier patches v9.15.2.59 and v10.3.4.0 did not fully address either flaw.
- The vendor says partners on affected v10 versions should apply the v10.3.4.45 hotfix.
- The vendor says partners on affected v7, v8 and v9 versions should apply the v9.15.2.70 hotfix.
- The vendor says to reboot the server after applying the hotfix. Its hotfix downloads need a partner portal login.

Things people will get wrong

- "We patched last time, so we are fine." The vendor says the earlier patches 9.15.2.59 and 10.3.4.0 did not fully address this flaw. Only the hotfix versions are named as fixes.
- "A 7.5 score means this can wait." The record's 7.5 is a CVSS 2.0 score. CISA lists the flaw as exploited, the record says the exploit is public, and CISA says it chains with CVE-2026-105134.
- "It is only a backup server, so it is low value." The sources do not say what an attacker gains after the bypass. Treat any login bypass on a server holding backups as serious until your provider says otherwise.

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

- Ask your IT provider whether AhsayCBS is used, where, and on which version.
- Check the version in the AhsayCBS web console or on the server. Compare it with 9.15.2.69 and 10.3.4.44.

```
ps aux | grep -i [a]hsay
ss -tlnp | grep -i java
```

Step 2: Reduce exposure

- If the server faces the internet, restrict access to trusted addresses until it is patched. The record says the attack works remotely.

Step 3: Apply the vendor's hotfix

- Use 9.15.2.70 for v7, v8 and v9, or 10.3.4.45 for v10. The vendor says these need a partner portal login.
- Reboot the server afterwards, as the vendor says.

Step 4: Check and look for signs of use

- Confirm the running version is the hotfix version.
- Review access logs for unexpected logins or API calls to checkSysPwd, from before and after 4 October 2026.

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-2026-105133 in AhsayCBS, which CISA lists as exploited. Please tell us whether we run AhsayCBS, where, and which version. The vendor says hotfix 9.15.2.70 (v7, v8, v9) or 10.3.4.45 (v10) fixes it, and that earlier patches did not. CISA's deadline was 17 October 2026. Please confirm in writing the version and that the hotfix is applied and the server rebooted, by a date you suggest, and tell us if you found signs of misuse. 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:

- Logins or API requests to the AhsayCBS API that did not come from your own staff or tools.
- Requests to the checkSysPwd function with unusual random values, in web or application logs.
- New or changed administrator accounts, settings or backup jobs you did not make.

The weakness behind it

The record classes this as CWE-287 (Improper Authentication).

The sources, in their words

CISA's catalogue entry:

> *Ahsay AhsayCBS contains an improper authentication vulnerability that could allow a remote attacker to bypass authentication via manipulation of the random parameter in the API component's checkSysPwd function. This vulnerability can be chained with CVE-2026-105134.*

The CVE record, published by VulDB on 4 October 2026:

> *A vulnerability was detected in Ahsay AhsayCBS up to 9.15.2.69/10.3.4.44. This affects the function checkSysPwd of the file com/ahsay/obs/api/ApiStructsAction.java of the component API. Performing a manipulation of the argument random results in improper authentication. It is possible to initiate the attack remotely. The exploit is now public and may be used. Upgrading to version 9.15.2.70 and 10.3.4.45 is able to mitigate this issue. It is recommended to upgrade the affected component. The initial patch did not fix the security vulnerability properly. An update of the CVE entry to reflect this became necessary.*

The record lists 115 affected versions or ranges of AhsayCBS. The first 8 are below; the rest are in the CVE record, so check your version against the whole list.

- 9.15.2.0
- 9.15.2.1
- 9.15.2.2
- 9.15.2.3
- 9.15.2.4
- 9.15.2.5
- 9.15.2.6
- 9.15.2.7

It lists these as unaffected:

- 9.15.2.70
- 10.3.4.45

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

- The sources do not say what an attacker can do on the server once past the login.
- The sources do not say which versions between those listed are affected beyond 'up to 9.15.2.69/10.3.4.44'.
- The sources do not say whether the hotfix is available to customers without a partner portal account.
- The sources do not describe how CVE-2026-105134 is chained with this flaw.
- 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. Timeline

Date	Event

4 October 2026	CVE record published by VulDB.
14 October 2026	CISA added it to its list of exploited vulnerabilities.
17 October 2026	CISA's deadline for US federal agencies.

Appendix 2. Exposure by situation

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

Your situation	Priority	Timeframe
AhsayCBS on an affected version, reachable from the internet	High	Now; CISA's date has passed
AhsayCBS on an affected version, reachable only from an internal network	High	This week
AhsayCBS patched with 9.15.2.59 or 10.3.4.0 only	High	Now; the vendor says these did not fully fix it
AhsayCBS already on 9.15.2.70 or 10.3.4.45	Low	Confirm the version in writing
You do not run AhsayCBS	None	None for this CVE

Appendix 3. Definition of done

- Every AhsayCBS 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-2026-105133: https://www.cve.org/CVERecord?id=CVE-2026-105133
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.ahsay.com/en/company/announcements/patch-cve-105133-10513: https://www.ahsay.com/en/company/announcements/patch-cve-105133-105134-update
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/413350
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/413350/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-105133
- Reference in the CVE record: vuldb.com: https://vuldb.com/submit/942688