contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

AhsayCBS exploited

CVE-2026-105134 · on CISA's exploited list since 14 October 2026

Analysis Report

If you run AhsayCBS, act now: CISA's date of 17 October 2026 has already passed. Check your version, and if it is below 9.15.2.70 or 10.3.4.45, ask your provider for the vendor hotfix today. If you …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	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-2026-105134

The bottom line

> *If you run AhsayCBS, act now: CISA's date of 17 October 2026 has already passed. Check your version, and if it is below 9.15.2.70 or 10.3.4.45, ask your provider for the vendor hotfix today. If you do not run AhsayCBS, you can stop reading.*

At a glance

Fact	Detail
Product	AhsayCBS (CVE-2026-105134)
Severity	Critical: 10 (CVSS 4.0)
CISA	On its exploited list since 14 October 2026. Deadline for US federal agencies: 17 October 2026.
Chance of exploitation (EPSS)	0.82, 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	AhsayCBS 9.15.2.70 and 10.3.4.45 (vendor hotfix, partner login required, reboot after applying; advisory of 12 October 2026).
Who looks first	Anyone running AhsayCBS on v7, v8, v9 or v10 up to 9.15.2.69 or 10.3.4.44, including IT providers who host it for clients. The record says the attack can be launched remotely.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run AhsayCBS, yourselves or through a provider?	Nothing to do for this CVE.	Check the version (next question).
Is your version 9.15.2.69 or 10.3.4.44 or earlier?	At 9.15.2.70 or 10.3.4.45 or later, this flaw is fixed. Keep the proof.	You are affected. Ask for the hotfix now.
Is the server reachable from the internet or from networks you do not control?	Lower exposure, but still patch. The record says the attack is remote.	Restrict access at once, then patch.

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

What it is

The record says a remote attacker can run operating system commands on the server. They do it by manipulating the random parameter of the Replication Receiver's UpdateReceivers endpoint. CISA says it can be chained with CVE-2026-105133.

Why it matters

Our reading is that a backup server is a valuable place for an attacker to get command execution. It holds client data and the credentials used to reach it. The record gives a score of 10 under CVSS 4.0 and says the exploit has been published. The vendor says its first patches did not fully fix the flaw, so a server patched earlier may still be open. Its hotfix is partner-only, so an owner without a partner login must go through their provider.

What the vendor's advisory says

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

- The vendor's advisory of 12 October 2026 says its earlier patches v9.15.2.59 and v10.3.4.0 did not fully address CVE-2026-105133 and CVE-2026-105134.
- 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.
- The vendor says a valid partner portal login is needed to download the hotfix.

Things people will get wrong

- "We patched when the first fix came out, so we are covered." The vendor says its earlier patches v9.15.2.59 and v10.3.4.0 did not fully address this flaw. You need 9.15.2.70 or 10.3.4.45.
- "This only affects v10." The vendor tells partners on affected v7, v8 and v9 versions to apply the 9.15.2.70 hotfix. The record lists 9.15.2 versions as affected.
- "We can download the fix ourselves." The vendor says the hotfix needs a valid partner portal login. Ask your provider or the vendor.
- "The hotfix is live as soon as it is installed." The vendor says to reboot the server after applying the hotfix.

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 who runs AhsayCBS for you, and where. Include test and old servers.
- Read the version in the AhsayCBS web console, and compare it with 9.15.2.70 and 10.3.4.45.

```
ps -ef | grep -i [c]bs
```

Step 2: Reduce exposure

- Limit access to the server to the networks that need it, until the hotfix is in. The record says the attack is remote.
- List what is listening on the server so you know what is reachable.

```
ss -tlnp
```

Step 3: Apply the vendor hotfix

- Ask your provider to apply 9.15.2.70 (v7 to v9) or 10.3.4.45 (v10) from the vendor's partner portal.
- Reboot the server afterwards, as the vendor says.

Step 4: Confirm the fix and look for misuse

- Get written confirmation of the running version after the reboot.
- Ask your provider to check the server for signs of misuse from before the fix.

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 know whether we run AhsayCBS, and where, including any test or old servers. Please tell us the version of each. CVE-2026-105134 is a command injection flaw in AhsayCBS. The vendor says versions up to 9.15.2.69 and 10.3.4.44 are affected, and its earlier patches did not fully fix it. Please apply the vendor's hotfix (9.15.2.70 or 10.3.4.45), reboot the server, and confirm in writing the running version. CISA's date for this was 17 October 2026, so please reply by Friday. Please also tell us whether the server was reachable from the internet.*

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 commands or new processes started by the AhsayCBS service on the server.
- Requests to the UpdateReceivers endpoint from addresses you do not recognise, with odd values in the random parameter.
- New accounts, scheduled tasks or changes to backup settings that nobody on your side made.

The weakness behind it

The record classes this as CWE-78 (Improper Neutralization of Special Elements used in an OS Command) and CWE-77 (Improper Neutralization of Special Elements used in a Command).

The sources, in their words

CISA's catalogue entry:

> *Ahsay AhsayCBS contains a command injection vulnerability that could allow a remote attacker to execute operating system commands via manipulation of the random parameter in the Replication Receiver component's /rps/api/json/UpdateReceivers.do endpoint. This vulnerability can be chained with CVE-2026-105133.*

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

> *A flaw has been found in Ahsay AhsayCBS up to 9.15.2.69/10.3.4.44. This vulnerability affects unknown code of the file /rps/api/json/UpdateReceivers.do of the component Replication Receiver. Executing a manipulation of the argument random can lead to os command injection. It is possible to launch the attack remotely. The exploit has been published and may be used. Upgrading to version 9.15.2.70 and 10.3.4.45 is able to resolve this issue. Upgrading the affected component is advised. 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 whether the attacker needs a login, or whether the endpoint is on by default.
- The sources do not say which other products or components are affected beyond AhsayCBS.
- The sources do not describe what an attacker has done with this flaw in practice.
- The sources do not say how to check for signs of compromise, or whether a workaround exists besides the hotfix.
- 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-2026-105134: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A`
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	None	No one has to do anything.
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
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 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

AhsayCBS at or below 9.15.2.69 or 10.3.4.44, reachable from the internet	High	Now; CISA's date has passed
Affected version, reachable only from an internal network	High	This week, after restricting access
You patched earlier with 9.15.2.59 or 10.3.4.0 and nothing since	High	Now; the vendor says that patch was incomplete
Hotfix applied but the server was not rebooted	Medium	At the next safe window, this week
You do not run AhsayCBS	None	None for this CVE

Appendix 4. 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-2026-105134: https://www.cve.org/CVERecord?id=CVE-2026-105134
- 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/413351
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/413351/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-105134
- Reference in the CVE record: vuldb.com: https://vuldb.com/submit/942743