

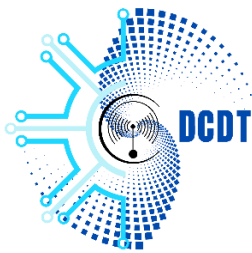
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

15 October 2026

Advisory 356: Ahsay AhsayCBS Authentication Bypass and Remote Code Execution Vulnerabilities - Actively Exploited (CVE-2026-105133 and CVE-2026-105134).

Release Date: 14th October 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-105133 and CVE-2026-105134 are two vulnerabilities in AhsayCBS, the central management console of the Ahsay backup platform, that attackers are chaining to get unauthenticated remote code execution with SYSTEM privileges. CVE-2026-105133 is an authentication bypass in the console's API (the password check is skipped when a request carries a specific flag), and CVE-2026-105134 is a flaw in the Replication Receiver component that lets an attacker run operating system commands or write files such as a JSP web shell into a web-served directory. Exploitation of CVE-2026-105134 requires the server to be configured or licensed as a replication receiver. Because the two flaws are used together, CERTVU has combined them in one advisory.

What are the systems affected?

The following Ahsay AhsayCBS versions are affected:

- AhsayCBS v10 builds before hotfix 10.3.4.45, including 10.3.4.0 (NVD lists versions up to 10.3.2, but Ahsay and Huntress confirm 10.3.4.0 is also vulnerable)

- AhsayCBS v9 builds before hotfix 9.15.2.70, including 9.15.2.59
- AhsayCBS v7 and v8, which must be upgraded to v9

The hotfixes are downloaded through the Ahsay partner portal. Treat any build below these as exposed.

Not affected / patched version:

- v10: hotfix 10.3.4.45, then reboot
- v9: hotfix 9.15.2.70, then reboot
- v7 or v8: upgrade to 9.15.0.0, then apply hotfix 9.15.2.70

What does this mean?

Successful exploitation may allow attackers to:

- Bypass login to the backup console and run commands as SYSTEM on the server without credentials
- Install web shells, cryptominers and persistence, and take over the server that stores backup data and credentials
- Read, delete or encrypt backups, which can remove an organization's ability to recover from ransomware, and use the server as a foothold into the network

Mitigation process

CERTVU recommends the following:

1. Apply the Ahsay hotfix

Apply hotfix 10.3.4.45 (v10) or 9.15.2.70 (v9) and reboot, or upgrade v7/v8 to 9.15.0.0 first. If you cannot get partner portal access, contact Ahsay or your reseller at once.

2. Restrict access to the console

Limit the AhsayCBS management interface to trusted IP addresses or a VPN, and do not expose it to the internet.

3. Hunt for compromise

4. Block known malicious infrastructure

5. Rebuild if compromised

Reference

1. <https://horizon3.ai/attack-research/vulnerabilities/cve-2026-105133-and-cve-2026-105134/>
2. <https://www.securityweek.com/unpatched-ahsaycbs-vulnerabilities-exploited-in-the-wild/>
3. <https://thehackernews.com/2026/10/attackers-exploit-ahsaycbs-flaws-to.html>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>