

Ahsay releases new fixes for AhsayCBS flaws exploited to drop web shells



Ahsay Backup has issued updates for two AhsayCBS flaws, CVE-2026-105133 and CVE-2026-105134, exploited to deploy web shells and XMRig miners. The source says earlier patches were incomplete.

- Ahsay Backup, based in Singapore, released security updates for AhsayCBS.
- The flaws are CVE-2026-105133 and CVE-2026-105134.
- Chained together, they can bypass authentication and run arbitrary commands.
- Attackers have used them to drop web shells and XMRig cryptocurrency miners.
- The new fixes follow earlier patches that proved incomplete.

Ahsay Backup, a Singapore-based vendor, has released new security updates for AhsayCBS, its backup management platform. The updates address two vulnerabilities, CVE-2026-105133 and CVE-2026-105134, which attackers have already exploited.

What is known

According to the report, the two flaws can be chained to sidestep authentication and then execute arbitrary commands on an affected system. Threat actors have used this path to place web shells and XMRig cryptocurrency miners on compromised servers. The headline indicates that the new fixes were needed because earlier patches did not fully close the issues.

The source excerpt does not provide further technical detail, affected version numbers or the scale of exploitation, so organisations should consult the vendor's own advisory for those specifics.

Why it matters

Backup platforms hold privileged access and copies of sensitive data, which makes a compromise there more serious than on an ordinary server. A web shell gives an attacker a persistent foothold, so patching alone may not remove an intruder who is already present. The fact that earlier patches were incomplete also means that teams who applied them should not assume they are protected.

Recommended approach

Treat this as a patch-and-verify exercise: confirm the exact version you run, apply the latest vendor update, and check for signs of prior compromise before returning the system to normal operation.

What to do now

1. Identify all AhsayCBS instances in your environment, including those managed by third parties.
2. Apply the latest Ahsay update even if earlier patches were installed, and confirm the resulting version.
3. Hunt for web shells and XMRig miner processes on AhsayCBS servers before and after patching.
4. Restrict management interface access to trusted internal networks and avoid direct internet exposure.
5. Review backup integrity and rotate administrative credentials if compromise is suspected.