TransilienceAI

CVE-2026-105134

Vulnerability Report · TLP:CLEAR

Ahsay · AhsayCBS

22 Nov 2026

Version 426 · 3 sources

TLP:CLEAR — Transilience Newsroom

Compiled by Transilience from public reporting. May be shared without restriction.

Table of Contents

BRIEF . . . 3

- Bottom line . . . 3
- For the board . . . 3
- Are you exposed? . . . 3
- What to do . . . 3

TIMELINE . . . 4

AFFECTED PRODUCTS AND VERSIONS . . . 4

FIXED IN . . . 4

EXPLOITATION . . . 4

WHO IS EXPLOITING IT . . . 4

MITIGATIONS AND DETECTION . . . 5

ATT&CK; TECHNIQUES . . . 5

INDICATORS . . . 5

NOT KNOWN YET . . . 5

SOURCES . . . 5

ABOUT THIS REPORT . . . 5

Brief

UNCLEAR — “EXPLOITED IN THE WILD” IS NOT SHOWN BY A QUOTE
—

Bottom line

Threat actors chained an auth bypass and unauthenticated SYSTEM RCE in AhsayCBS to plant webshells, miners and a sandbox-aware Python backdoor; hotfixes block entry but do not remove implants — hunt for artifacts and reimage exposed backup servers immediately. [1,2,3]

For the board

Threat actors exploited AhsayCBS to install persistent miners and backdoors; patching prevents new exploits but does not remove implants—search and reimage exposed backup servers.

Are you exposed?

Affects	How to check
Ahsay · AhsayCBS — versions before the fixed releases [1,3]	Check AhsayCBS product version in Admin Console or installer metadata; compare to 10.3.4.45 / 9.15.2.70.

What to do

1. **Install Ahsay hotfixes (10.3.4.45 for v10; 9.15.2.70 for v7–v9).** [1,3]
   These hotfixes block the observed entry point used in the intrusions.
2. **Hunt for implanted artifacts (JSP webshells, kvm scheduled task, SYSTEM Python).** [1,3]
   Patching does not remove backdoors, scheduled tasks, or implants already planted.
3. **Reimage any compromised or exposed backup servers from trusted backups.** [1,3]
   Remediation gap: fixes block entry but do not remove existing implants; reimaging removes persistence.
4. **Look for indicators: unexpected JSP files, Defender exclusions, unusual cbssvcX64.exe activity.** [3]
   These artifacts and behaviours were present on compromised systems and aid detection and cleanup.

Timeline

Date	Kind	What happened
between October 8 and October 11, 2026	EXPLOITATION	Servers in the investigated environment were exploited [1] *“The impacted organization's servers in this post were exploited between October 8 and October 11, 2026, which was before Ahsay released its hotfixes.”* [1]
October 12, 2026	PATCH	Ahsay released hotfixes [1] *“Ahsay has since released hotfixes (10.3.4.45 for v10, and 9.15.2.70 for v7 through v9), and we verified that 10.3.4.45 blocks the entry point we saw.”* [1]
2026-11-10 published	DISCLOSURE	Follow-up reporting on sandbox-evading Python backdoor [2] *“The notable aspect of the intrusion revolves around the Python backdoor ("main.py"), which is designed to run only on the host it's staged on and prevent it from executing within a sandbox or an analyst's machine.”* [2]
2026-11-11 published	DISCLOSURE	Summary published detailing persistence and remediation gap [3] *“The findings underscore a remediation gap: installing security hotfixes blocks the observed entry point but does not remove previously planted backdoors, scheduled tasks, or implants.”* [3]

Affected products and versions

The sources do not list affected versions.

Fixed in

- 10.3.4.45 for v10; 9.15.2.70 for v7 through v9 [1]
  “Ahsay has since released hotfixes (10.3.4.45 for v10, and 9.15.2.70 for v7 through v9), and we verified that 10.3.4.45 blocks the entry point we saw.” [1]

Exploitation

- Exploitation in the wild observed in early October against AhsayCBS servers [1]
  “The impacted organization's servers in this post were exploited between October 8 and October 11, 2026, which was before Ahsay released its hotfixes.” [1]
- Campaign deployed webshells, miners, tunneling tools, and a Python backdoor [3]
  “Attackers exploiting AhsayCBS backup servers deployed five webshell families, persistent cryptocurrency miners, tunneling utilities, and a custom Python implant across three servers in one organization.” [3]

Who is exploiting it

- Unknown / unnamed threat actor [2]
  “Specifically, the unknown threat actor is said to have left five families of Jakarta Server Pages (JSP, formerly JavaServer Pages) web shells -” [2]

Mitigations and detection

- Install hotfixes; verify they block observed entry point. [1]
  “Ahsay has since released hotfixes (10.3.4.45 for v10, and 9.15.2.70 for v7 through v9), and we verified that 10.3.4.45 blocks the entry point we saw.” [1]
- Search for JSP files, SYSTEM-profile Python installations, unauthorized tasks, Defender exclusions. [3]
  “Defenders should examine unexpected JSP files, SYSTEM-profile Python installations, unauthorized tasks, Defender exclusions, and commands spawned by cbssvcX64.exe.” [3]
- Reimage compromised hosts from trusted backups rather than relying on patching alone. [3]
  “Huntress’s original report provides campaign indicators and Sigma detection guidance, and recommends reimaging compromised hosts from trusted backups rather than relying on patching alone.” [3]

ATT&CK techniques

The sources do not describe the attacker's behaviour closely enough to map.

Indicators

Kind	Indicator
URL	`hxxps://creepexplosiondarknight[.` [1]
DOMAIN	`creepexplosiondarknight[.]com` [1]

Not known yet

- Total number of affected customers or servers
- Whether backup credentials were successfully exfiltrated
- Attribution of the threat actor
- Any KEV listing or CISA advisory

Sources

#	Outlet	Article	Copy
1	**Huntress blog** 9 Nov 2026	Inside an AhsayCBS Intrusion: Hidden Webshells, a CryptoMiner, and a C2 Implant | Huntress	archived copy
2	**The Hacker News** 10 Nov 2026	Attackers Exploit AhsayCBS Flaws to Deploy Sandbox-Evading Python Backdoor	archived copy
3	**GBHackers** 11 Nov 2026	AhsayCBS Hackers Plant Multiple Webshells and Secret Crypto Miners That Survive Security Patching	archived copy

About this report

Compiled by Transilience Newsroom from 3 public sources. Every quotation is checked against the article it cites; 9 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 426, written 22 November 2026, 13:31 UTC (cve-report-2026-09-25c). TLP:CLEAR — may be shared without restriction. The live report: https://threatnews.transilience.cloud/report/cve/cve-2026-105134