Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

AhsayCBS Zero-Days Turn MSPs Into Crypto Mines

Date of Publication	Last Update Date	Admiralty Code	TA Number
October 12, 2026	October 16, 2026	A1	TA2026296

Summary

First Seen: October 4, 2026
Malware: XMRig, JSP Webshell
Affected Product: Ahsay AhsayCBS
Impact: AhsayCBS is the backup console that managed service providers use to run backups for their customers, and two flaws in it are under active attack. CVE-2026-105133 is a broken login check, and CVE-2026-105134 allows operating system commands through the Replication Receiver component. Chained together, they give anyone on the internet remote code execution with full SYSTEM rights. The first attacks occurred on October 7, 2026, three days after the CVEs were published, and counted five affected organisations within a day. The attackers dropped JSP webshells and an XMRig Monero miner renamed edge.exe to pass for Microsoft Edge, kept running by a service called MicrosoftEdgeUpdateSvc and hidden by a script that pauses mining whenever Task Manager is open. The fix has already changed once: 10.3.4 was listed as the safe version but was not, and Ahsay released hotfix v10.3.4.45 and v9.15.2.70.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-105133	Ahsay AhsayCBS Improper Authentication Vulnerability	Ahsay AhsayCBS	✓	✓	✓
CVE-2026-105134	Ahsay AhsayCBS Command Injection Vulnerability	Ahsay AhsayCBS	✓	✓	✓

Vulnerability Details

#1

The two flaws fall into different classes but were built to work together. CVE-2026-105133 is an improper authentication issue (CWE-287) in the checkSysPwd() function of com/ahsay/obs/api/ApiStructsAction.java. The function is meant to confirm that a caller holds valid system credentials, but it can be satisfied without them, so an unauthenticated request is treated as a trusted one. CVE-2026-105134 is an operating system command injection issue, mapping to CWE-78, in the Replication Receiver component exposed at /rps/api/json/UpdateReceivers.do. That API carries an authentication bypass of its own, where a random token can stand in for valid credentials, and it accepts input that reaches the underlying operating system shell.

#2

In practice, the attackers chain them. The authentication weakness is used first to get past the login check, and the command injection is then used to run code on the host as NT AUTHORITY/SYSTEM. The entry point is the AhsayCBS web management interface, which is reachable from the internet on many deployments because that is how administrators and remote sites are expected to connect. No credentials, user interaction, or prior foothold are needed, which is what makes the chain so attractive for mass scanning. The first sign on a compromised host is usually an unexpected child process spawning from the AhsayCBS service binary, cbssvcX64.exe, because the web application runs inside that service process and anything an uploaded webshell executes appears underneath it.

#3

AhsayCBS versions up to and including 10.3.4 are affected. Ahsay then issued its own notice on October 10 stating that build v10.3.4.0 did not fully address either vulnerability, and released hotfix v10.3.4.45 as the corrected build, to be applied from the partner portal and followed by a server reboot. Ahsay has described the affected scope only as affected v10 versions without naming specific builds, so until the vendor publishes an exact list, every v10 deployment below hotfix 10.3.4.45 should be treated as exposed. They have also released v9.15.2.70 hotfix for users affected by versions v7, v8, and v9.

#4

Active exploitation is confirmed, not theoretical. Observing attacks on October 7, 2026 at 23:20:15 UTC, roughly 72 hours after publication, and identified five targeted organisations by October 8, with one further incident reported afterwards using the same techniques. The post-exploitation activity is consistent across victims: JSP webshells written into the web application directory, payloads retrieved into %TEMP% or AppData\Local\Temp using curl and certutil.exe, an XMRig miner connecting to a Monero pool on port 8029, a Windows service named to imitate Microsoft Edge Update for persistence, and a Task Manager-aware PowerShell script to hide the activity from anyone watching.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-105133	Ahsay AhsayCBS (v10 builds before hotfix 10.3.4.45)	cpe:2.3:a:ahsay:ahsaycbs:*:*:*:*:*:*:*:*	CWE-287
CVE-2026-105134	Ahsay AhsayCBS (v10 builds before hotfix 10.3.4.45)	cpe:2.3:a:ahsay:ahsaycbs:*:*:*:*:*:*:*:*	CWE-77 CWE-78

Recommendations

Apply Hotfix v10.3.4.45, v9.15.2.70, and reboot: Ahsay has confirmed that its earlier v10.3.4.0 build did not fully address either CVE and has released hotfix v10.3.4.45 (v10 versions) and v9.15.2.70 (v7, v8, and v9 versions) as the real fix. Download it from the Ahsay partner portal, apply it to every AhsayCBS server, and reboot the host afterwards, since the vendor states the reboot is part of the remediation. If you consume AhsayCBS through a service provider, ask them directly for the exact build number running on your console.

Hunt for the Indicators Before Assuming You Are Clean: Check your AhsayCBS hosts for the indicators listed in this advisory, including the payload hosting URLs, the miner and NSSM file hashes, the MicrosoftEdgeUpdateSvc service and newly written .jsp files in the web application directory. Also review process telemetry for any child process spawning from cbssvcX64.exe or cbssvcX86.exe that is not part of the service's normal startup and maintenance behaviour.

Take the Management Interface Off the Internet: The exploit targets the externally accessible web application service on the host, so restrict web access to the AhsayCBS management interface to a short list of trusted IP addresses or require VPN. Keep this control in place even after the hotfix is applied, because it removes the attack path for the next flaw in the same interface rather than just this one.

Block the Mining and Payload Infrastructure: Add the listed IP addresses, the Alibaba Cloud payload hosting domain and the Monero pool to your egress blocklists, and alert on outbound connections to non-standard ports such as 8029. Cryptomining needs a working outbound channel, so egress control both limits the damage and gives you a reliable detection signal.

Watch for Vulnerable Driver Loads: The campaign loads WinRing0x64.sys, a legitimate but vulnerable kernel driver, to give the miner low-level hardware access. Enable Microsoft's vulnerable driver blocklist where you can, and alert on driver files being written into temporary folders or loaded from user-writable paths.

Treat Backup Infrastructure as Tier 0: Backup consoles hold the keys to recovery and, for service providers, to many customer environments at once. Give them the same isolation, monitoring and administrative controls as domain controllers, keep them off the public internet by default, and make sure at least one backup copy is offline and outside the reach of the console itself.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1608: Stage Capabilities	T1608.001: Upload Malware
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
	T1569: System Services	T1569.002: Service Execution

Tactic	Technique	Sub-technique
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
Privilege Escalation	T1543: Create or Modify System Process	T1543.003: Windows Service
Defense Evasion	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Resource Name or Location
	T1564: Hide Artifacts	
Discovery	T1057: Process Discovery	
	T1124: System Time Discovery	
Command and Control	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1571: Non-Standard Port	
Impact	T1496: Resource Hijacking	T1496.001: Compute Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	05f69ae6b2b89c1c4dcf836bff032232f11bf0109f2b498e2345045d06139034, 4dcb0202fe8b2d4d7b183764e38184cd6ed50132786cc7e7d1f7f4bce1dd6f3d, 481728a7c9c4c02be07051d9c1958d902ea6397ebb8952ab83944818e3d25d21
IPv4	177[.]4[.]12[.]11, 38[.]60[.]252[.]110, 107[.]191[.]47[.]199, 185[.]220[.]236[.]49, 104[.]234[.]26[.]10, 123[.]202[.]208[.]37
IPv4:Port	51[.]195[.]127[.]124[:]8029
Domains	imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com, xmr[.]kryptex[.]network
URLs	hxxp[:]//imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/javas/Office/win/Taskgmr[.]ps1, hxxp[:]//imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/javas/Office/win/edge[.]exe, hxxp[:]//imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/javas/Office/win/msedge[.]exe, hxxp[:]//imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/javas/Office/win/config[.]json, hxxp[:]//imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/javas/Office/win/WinRing0x64[.]sys
Mining Pool User	krxYMRN97D/creativejs

Patch Link

https://idp3.ahsay.com/idp/Authn/RemoteUser

References

https://www.huntress.com/blog/ahsaycbs-flaws-exploit

https://www.ahsay.com/en/company/announcements/patch-cve-105133-105134

https://www.ahsay.com/en/company/announcements/patch-cve-105133-105134-update

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

October 12, 2026 • 08:45 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com