

Critical Command Injection Vulnerability in Ahsay AhsayCBS Backup Platform



A critical command injection vulnerability in Ahsay AhsayCBS allows remote attackers to execute operating system commands through the Replication Receiver component, requiring immediate patching.

- CVE-2026-105134 affects Ahsay AhsayCBS backup platform with a command injection flaw in the Replication Receiver component
- Attackers can exploit the vulnerability remotely via the random parameter in the `/rps/api/json/UpdateReceivers.do` endpoint
- The vulnerability can be chained with CVE-2026-105133 for potentially greater impact
- Organizations must apply vendor patches immediately or discontinue product use if mitigations are unavailable

- CISA has set a federal remediation deadline of 17 October 2026 under BOD 26-04 guidance

Vulnerability Overview

Ahsay AhsayCBS, a widely deployed backup and disaster recovery platform, contains a critical **command injection vulnerability** tracked as CVE-2026-105134. The flaw resides in the Replication Receiver component and allows remote attackers to execute arbitrary operating system commands by manipulating the random parameter in the `/rps/api/json/UpdateReceivers.do` endpoint. This vulnerability requires no authentication and can be exploited remotely, presenting significant risk to organizations relying on this platform for business continuity.

The vulnerability can be chained with CVE-2026-105133, potentially amplifying the attack surface and impact. Command injection flaws of this nature enable attackers to gain unauthorized access to underlying systems, exfiltrate sensitive data, deploy ransomware, or establish persistent backdoors within enterprise networks.

Regulatory and Compliance Context

CISA has issued guidance under BOD 26-04 Prioritizing Security Updates Based on Risk, establishing a federal remediation deadline of 17 October 2026. While this directive applies to US federal agencies, regulated institutions in Saudi Arabia should treat this timeline as a benchmark for urgent action. Organizations subject to NCA cybersecurity controls or SAMA frameworks must evaluate their exposure and implement mitigations promptly to maintain compliance with mandatory security baselines.

Immediate Response Requirements

Organizations must immediately identify all instances of Ahsay AhsayCBS within their environment, particularly internet-facing deployments. Apply vendor-supplied patches as soon as they become available. If mitigations are not yet released or cannot be applied, consider isolating affected systems from network access or discontinuing use until remediation is possible. Document all remediation activities for audit purposes and conduct forensic triage if any indicators of compromise are detected.

What to do now

1. Conduct an immediate inventory of all Ahsay AhsayCBS installations across your environment, prioritizing internet-facing instances
2. Contact Ahsay vendor support to obtain security patches and implementation guidance for CVE-2026-105134 and CVE-2026-105133
3. Apply vendor-supplied patches immediately following change management procedures and testing protocols
4. If patches are unavailable, isolate affected systems from network access or discontinue use until mitigations are released

5. Review access logs and conduct forensic triage on affected systems to identify any indicators of compromise or unauthorized command execution
6. Document all remediation activities, including patch deployment dates and system configurations, for NCA or SAMA audit requirements