

Ahsay AhsayCBS Authentication Bypass Vulnerability Requires Immediate Patching



Ahsay AhsayCBS backup software contains an authentication bypass flaw allowing remote attackers to manipulate API parameters, requiring immediate vendor patches or service discontinuation.

- Improper authentication vulnerability in Ahsay AhsayCBS allows remote attackers to bypass authentication through API parameter manipulation
- The flaw affects the checkSysPwd function's random parameter in the API component
- Vulnerability can be chained with CVE-2026-105134 for potentially greater impact
- Organizations must apply vendor mitigations immediately or discontinue product use if patches unavailable
- Internet-exposed instances require priority assessment and remediation

Vulnerability Overview

Ahsay AhsayCBS, a backup and disaster recovery solution, contains an **improper authentication vulnerability** tracked as CVE-2026-105133. The flaw resides in the API component's checkSysPwd function, where attackers can manipulate the random parameter to bypass authentication mechanisms remotely. This vulnerability presents significant risk to organizations relying on the platform for backup operations, particularly when instances are exposed to the internet.

The vulnerability can be chained with CVE-2026-105134, potentially amplifying the impact of a successful exploit. Authentication bypass vulnerabilities are particularly concerning in backup systems, as they protect critical data assets and recovery capabilities that regulated institutions depend upon for business continuity.

Required Response Actions

Organizations using Ahsay AhsayCBS must apply vendor-supplied mitigations immediately in accordance with manufacturer instructions. Where patches or mitigations are not available, institutions should discontinue use of the product until secure alternatives can be implemented. This guidance aligns with risk-based security update prioritization principles.

Stakeholders are responsible for evaluating the internet exposure of each asset running the affected software. Systems accessible from external networks require immediate attention and remediation priority.

Organizations should conduct forensic triage where compromise is suspected.

Compliance Considerations

For Saudi regulated institutions, this vulnerability intersects with multiple compliance obligations. Backup system integrity directly supports business continuity requirements, while authentication controls are fundamental to access management frameworks. Organizations should document remediation activities and assess whether incident reporting thresholds have been met under applicable regulatory frameworks.

What to do now

1. Immediately inventory all instances of Ahsay AhsayCBS across your environment and assess internet exposure
2. Apply vendor-supplied security patches and mitigations according to manufacturer instructions without delay
3. If patches are unavailable, discontinue use of Ahsay AhsayCBS and implement alternative backup solutions
4. Conduct forensic triage on systems where unauthorized access is suspected, preserving logs and evidence
5. Review access logs for the checkSysPwd API function to identify potential exploitation attempts
6. Document all remediation activities and assess whether incident reporting obligations under NCA or sector regulators have been triggered