

ConnectWise resets credentials as Cloud Backup stays offline after security incident



ConnectWise says it is strengthening admin protections and resetting accounts and application credentials after unauthorized access to application identities tied to Cloud Backup, which remains offline.

- ConnectWise is responding to a security incident involving unauthorized access to application identities associated with Cloud Backup.
- Remediation includes stronger protection of administrative access.
- The company has reset accounts and replaced application credentials.
- The Cloud Backup service remains offline, according to the report.
- The source excerpt does not detail scope, affected customers or a restoration date.

ConnectWise has said it is continuing to respond to a security incident that led to unauthorized access to application identities associated with its Cloud Backup offering. The service remains offline.

What the company reports

On Monday the company described remediation measures taken so far. These include strengthening protections around administrative access, resetting accounts and replacing application credentials. The available source text is brief and does not list the full set of completed actions.

What is not yet known

The excerpt does not state how the access occurred, which customers or data are affected, or when Cloud Backup will return. Institutions should avoid assumptions and rely on direct communication from the vendor.

Why it matters for regulated institutions

Backup services hold copies of business-critical data, and application identities are credentials that let systems talk to each other. An incident involving them raises questions about credential exposure and about recovery readiness while the service is unavailable. Organisations that use ConnectWise Cloud Backup, directly or through a managed service provider, should confirm their position and make sure alternative recovery options exist.

What to do now

1. Confirm whether your organisation or any managed service provider uses ConnectWise Cloud Backup.
2. Ask the vendor or provider in writing about impact on your data and the expected restoration timeline.
3. Verify that you hold recent, tested backups outside the affected service.
4. Rotate any credentials or API keys you issued to integrate with the service, if applicable.
5. Review access logs for the integration for unusual activity and record the review for third-party risk files.