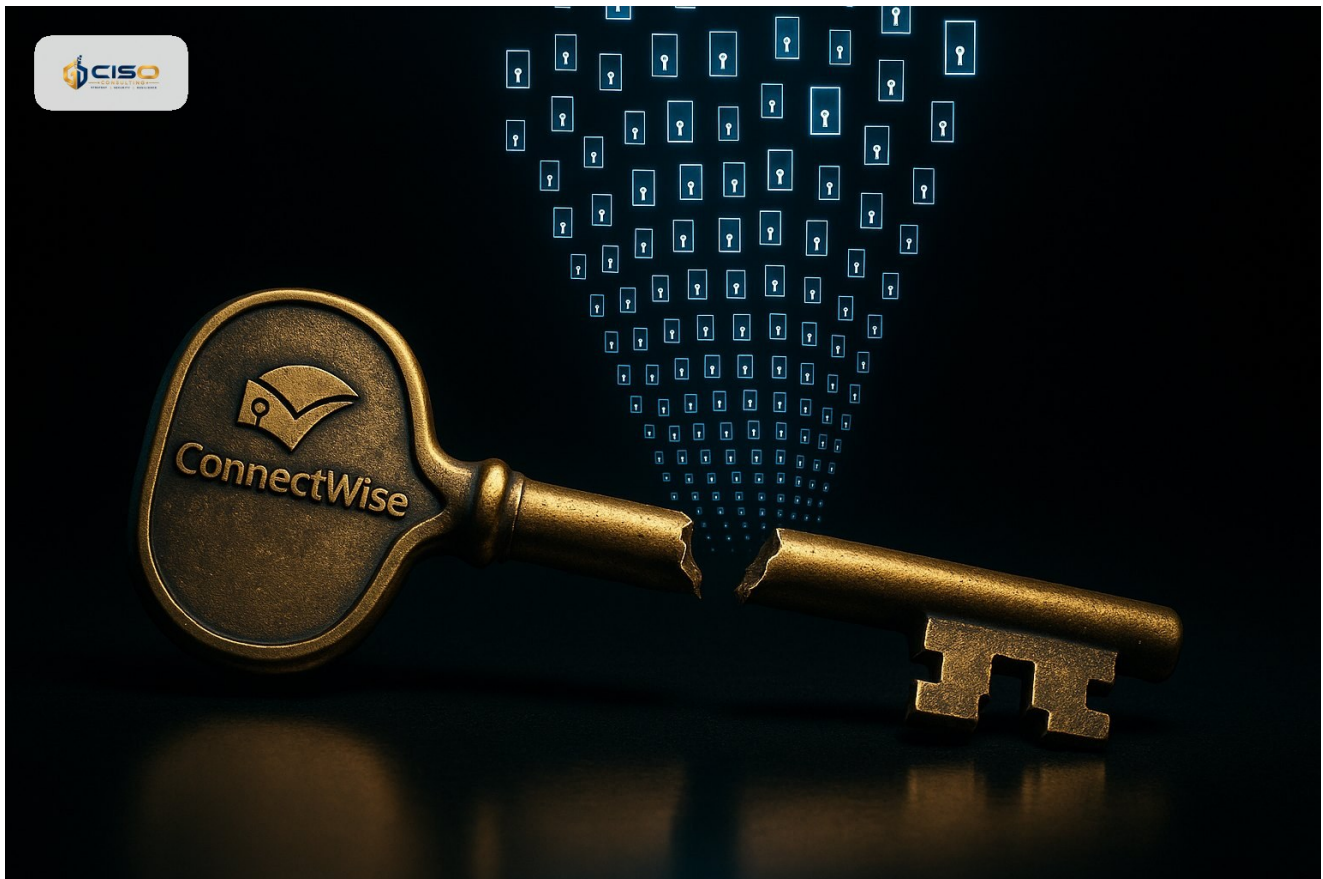


Compromised ConnectWise Credential Used to Access 173 Microsoft 365 Tenants



Threat actors exploited a compromised Microsoft 365 credential belonging to ConnectWise Cloud Backup to gain unauthorized access to 173 customer M365 environments in an active campaign.

- Unknown threat actors compromised a Microsoft 365 credential belonging to ConnectWise Cloud Backup service
- The compromised credential was used to access 173 customer Microsoft 365 tenants without authorization
- ConnectWise Cloud Backup is a cloud-based backup and recovery service used by managed service providers
- The campaign is currently active and under investigation by cybersecurity researchers

Incident Overview

Cybersecurity researchers have identified an active campaign in which threat actors exploited a compromised Microsoft 365 credential belonging to **ConnectWise Cloud Backup** to gain unauthorized access to customer environments. The service, formerly known as SkyKick, is a cloud-based backup and recovery platform designed for managed service providers. The compromised credential enabled attackers to sign in to 173 separate Microsoft 365 tenants belonging to ConnectWise customers.

Third-Party Access Risk

The incident highlights the risks associated with third-party service provider access to cloud environments. ConnectWise Cloud Backup requires privileged access to customer Microsoft 365 tenants to perform backup and recovery operations. When a single credential with broad access is compromised, threat actors can leverage that trust relationship to move laterally across multiple customer environments. The scale of the breach—173 affected tenants—demonstrates how a single point of compromise in a service provider's infrastructure can cascade across its entire customer base.

Current Status

The campaign remains active as researchers continue to investigate the scope and impact. Organizations using ConnectWise Cloud Backup or similar third-party services with delegated access to their Microsoft 365 environments should review access logs and authentication events for suspicious activity. The identity of the threat actors and their ultimate objectives have not been disclosed.

What to do now

1. Review all third-party service provider access to Microsoft 365 and other cloud platforms, documenting delegated permissions and privileged accounts
2. Audit authentication logs for Microsoft 365 tenants to identify any suspicious sign-in activity from ConnectWise Cloud Backup or other backup service credentials
3. Implement conditional access policies requiring multi-factor authentication for all service accounts with delegated access to cloud environments
4. Establish continuous monitoring of privileged third-party access, with alerts for unusual authentication patterns or access from unexpected locations
5. Review and update vendor risk management procedures to include regular access reviews and credential rotation requirements for managed service providers
6. Verify that backup and recovery service providers maintain separate credentials per customer rather than shared credentials with broad access