



One page, five minutes: what's happening in cybersecurity this week and what to do about it.

Provided by Major Business Solutions LLC

HEADLINE THREAT

ACTIVE INCIDENT

Hackers used stolen ConnectWise app credentials to get into Microsoft 365 accounts. ConnectWise Cloud Backup is offline.

Many IT providers use ConnectWise to manage and back up their clients' Microsoft 365. Attackers stole the credentials of seven ConnectWise apps that customers had already approved, and used them to sign in to customers' Microsoft 365 accounts. They didn't need anyone's password. The security firm Huntress saw sign-in attempts against nearly 1,000 Microsoft 365 organizations, about 300 of which succeeded. ConnectWise found the problem on Oct 14 and switched the apps off on Oct 17. Cloud Backup, SaaS Security and Cloud Management are still suspended, so **scheduled backups are not running and restores are unavailable**. ConnectWise says existing backup archives were not accessed.

Why it matters for you

If your IT provider uses ConnectWise, or you used SkyKick in the past, attackers may have been able to read your email, SharePoint and Teams. Turning the apps off doesn't remove anything an attacker set up while they were in, such as email forwarding rules, new admin accounts or extra app keys. Your Microsoft 365 backups may also have stopped without anyone telling you.

PATCH PRIORITY

VPN · KEV **Ivanti Connect Secure: CVE-2026-104935:** Lets an attacker take over the VPN without logging in. Exploited since early October and already being chained with a second flaw that gives full control, which Ivanti *hasn't fixed yet*. Update now, check for signs of compromise, and change any passwords stored on the device.

Remote support · KEV **BeyondTrust Remote Support: CVE-2026-102764** (CVSS 9.3): Exploited by a China-linked group since August. The cloud version is already patched. If you run it on your own server, install patch BT26-05-RS yourself. If that server was reachable from the internet, treat it as possibly compromised.

Firewall · KEV **Palo Alto PAN-OS: CVE-2026-0322:** Lets an attacker run code on firewalls through the admin login page. Update, and only allow the admin page to be reached from trusted internal addresses.

Email security · KEV **Cisco Secure Email Gateway: CVE-2026-76519** (CVSS 9.8): A booby-trapped email attachment can take over the device. Update Content Scanner Tools to 25.3.0.5525 or later.

Backup · KEV **AhsayCBS: CVE-2026-105133 / -105134**: Attackers are using these together to plant backdoors on backup servers. Earlier patches didn't fully fix them: install v10.3.4.45 or v9.15.2.70, then reboot.

CISA added six more exploited vulnerabilities to its catalog today (Oct 20). Have your IT provider check the list against what you run.

BY THE NUMBERS

~1,000

Microsoft 365 organizations targeted with the stolen ConnectWise app credentials (~300 sign-ins succeeded)

Huntress via The Hacker News, Oct 2026

2 of 3

flaws in the Ivanti VPN attack chain that are patched so far

Volexity via The Hacker News, Oct 2026

88%

of breaches at small and mid-size businesses involved ransomware (39% at large firms)

Verizon DBIR 2025 (Apr 2025)

12×

increase in phishing emails posing as quote requests and procurement inquiries

Fortra (Oct 2025–Sep 2026) via The Hacker News

THREE ACTIONS THIS WEEK

- 1. Ask your IT provider about ConnectWise today.** Ask whether you use ConnectWise Cloud Backup or Cloud Management, or used SkyKick in the past. If yes: check Microsoft 365 sign-ins since Oct 13, look for email forwarding rules, new admin accounts and new app keys, and keep the affected apps turned off. Also set up a temporary backup until the service comes back.
- 2. Patch your internet-facing equipment.** List your VPN, firewall, remote-support, email-security and backup servers, and confirm each one is on the fixed version above. Make sure admin login pages can't be reached from the internet. If a device was exposed and unpatched, have it checked for compromise; patching alone doesn't remove an attacker who is already in.
- 3. Brief staff on fake quote requests and fake downloads.** Phishing disguised as RFQs and project invitations is up sharply, and a fake WatchGuard VPN download site was recently caught stealing login details. Download software only from the vendor's official site, and confirm any change to payment details by calling a number you already have on file.



Provided by Major Business Solutions LLC

Sources

1. [The Hacker News: ConnectWise Suspends Cloud Backup After Attackers Compromise Microsoft 365 Tenants](#)
2. [Help Net Security: ConnectWise suspends Cloud Backup service \(Oct 19, 2026\)](#)

3. [CISA: Urges Patching Newly Exploited Vulnerability in Ivanti Connect Secure \(Oct 13, 2026\)](#)
4. [The Hacker News: Attacker Chains Three Ivanti Connect Secure Zero-Days](#)
5. [CISA: Urges Patching Critical Vulnerability in BeyondTrust Remote Support \(Oct 16, 2026\)](#)
6. [The Hacker News: China-Linked Hackers Exploited BeyondTrust Zero-Day](#)
7. [CISA: Adds Four Known Exploited Vulnerabilities to Catalog \(Oct 14, 2026\)](#)
8. [Help Net Security: CISA flags exploited flaws in Palo Alto, Cisco and Ahsay products](#)
9. [CISA: Adds Six Known Exploited Vulnerabilities to Catalog \(Oct 20, 2026\)](#)
10. [CISA: Known Exploited Vulnerabilities Catalog](#)
11. [The Hacker News: Weekly Recap \(Fortra phishing data, fake WatchGuard VPN site\)](#)
12. [The Record: Ransomware in nearly half of all data breaches \(Verizon DBIR 2025\)](#)

Advisories change quickly. Verify the current details directly with CISA (cisa.gov) and your vendors before acting.