It's Probably Nothing
by Sierra Echo Charlie

EDITION 04 / 19 OCTOBER 2026

One vendor credential, hundreds of M365 tenants

Plus an espionage zero-day in BeyondTrust, root-by-email on Cisco gateways, and a poisoned WordPress plugin.

5 stories / Listen online - 3:54

THE TAKEAWAY

A heavy window, so this runs longer than usual. The lead: a stolen credential for ConnectWise's Microsoft 365 backup app has been signing into customer tenants at scale. Also inside: an espionage actor's BeyondTrust zero-day, an exploited Cisco email gateway, and two short ones.

01 / THE BRIEF

A ConnectWise backup credential signed into hundreds of Microsoft 365 tenants

ConnectWise has confirmed that an API secret for Cloud Backup - the former SkyKick, an app consented into every customer tenant with read-write access to mail, files, chats and directory data - was compromised. Huntress watched the app's identity sign in from a rented hosting IP on 15 October, walking tenants in sorted GUID order seconds apart: a script working a list, basically. It confirmed unauthorised sign-ins in 162 tenants on 16 October; a day later it counted almost 1,000 tenants touched from that IP, more than 300 successfully. A second, targeted wave hit 16 tenants in policy, national-security, trade and critical minerals, most not ConnectWise customers. In one tenant, a second ConnectWise app granted itself Global Administrator and added credentials to two other applications, Huntress's own among them. Cloud Backup and two related services remain suspended, with no restore time given.

Microsoft, via BleepingComputer, calls it an active supply-chain attack. Data theft is unconfirmed because app reads barely log, so Huntress's 'tokens issued, nothing visible taken' is not the same as nothing taken.

WORTH ASKING

If you run tenants with ConnectWise or SkyKick apps consented: disable (don't delete) them, audit credentials added to any application since 13 October, and keep them off until ConnectWise confirms rotation. Issued tokens stay valid up to 90 minutes after disabling, so the switch isn't instant.

QUALIFICATIONS

How the credential escaped in the first place is still under investigation.

SOURCES

Compromised ConnectWise Backup Credential Enables Access to 162 Microsoft 365 Tenants - Reporting / context

ConnectWise (SkyKick) Vendor Credentials Abused in M365 Attacks | Huntress - Primary source

October 18, 2026: Cloud Backup (formerly known as SkyKick) Service Interruption | ConnectWise Trust Center - Primary source

Investigation: Unauthorized Access Through the ConnectWise Cloud Backup Microsoft 365 App | Todyl - Reporting / context

Hackers breach Microsoft 365 tenants via ConnectWise supply-chain attack (BleepingComputer) - Reporting / context

02 / THE BRIEF

ARMORY CASTLE had a BeyondTrust zero-day in August, and patching alone won't clear it

Mandiant says ARMORY CASTLE - the suspected PRC-nexus espionage actor formerly tracked as UNC5221 - exploited CVE-2026-102764 in BeyondTrust Remote Support as a zero-day from late August. It's a CVSS 9.3 affecting every supported version up to 26.2.3: unauthenticated file operations on the appliance, becoming host-level control of a box whose job is storing and brokering other people's credentials. Investigators found a webshell called SAWFLY, a SUID-root backdoor, dumps of the appliance credential vault and sudoers persistence that survives reboots and config resets, then a pivot through the Remote Support app itself with stolen admin credentials. CISA added it to KEV on 16 October with forensic triage attached; the federal due date is today.

Patching alone doesn't clear a compromised appliance, and customers can't audit the host filesystem. Mandiant warns mass exploitation may now follow disclosure, as it saw after this actor's Ivanti zero-days in 2024.

WORTH ASKING

Anything internet-reachable on a vulnerable version since August is potentially compromised: rebuild from known good and rotate everything the appliance ever held.

QUALIFICATIONS

The attribution is Mandiant's, and the vendor timeline (exploited 29 August, patch shipped 8 October) comes via SecurityWeek.

SOURCES

ARMORY CASTLE Exploits BeyondTrust Remote Support Zero-Day for Espionage - Reporting / context

ARMORY CASTLE Exploits BeyondTrust | Google Cloud Blog (Mandiant/GTIG) - Primary source

CISA Urges Patching Critical Vulnerability in BeyondTrust Remote Support | CISA - Primary source

Chinese APT Exploited BeyondTrust Vulnerability as Zero-Day (SecurityWeek) - Reporting / context

03 / THE BRIEF

Cisco's email gateway bug delivers root by email

CVE-2026-76519, CVSS 9.8, has the week's most pointed delivery path: email a crafted attachment through a Cisco Secure Email Gateway and, if AMP file reputation is on and Content Scanner Tools is older than 25.3.0.5525, you get arbitrary file writes and command execution as root on the box that scans the email. Cisco's PSIRT became aware of active exploitation in October; the bug surfaced in internal scanning. The fix is a Content Scanner Tools update with no restart, though the KEV deadline was 17 October, already gone.

WORTH ASKING

Root means the device's logs can lie, so cross-check external network logs; Cisco also wants cluster members that shared SSH keys with a compromised box rebuilt, and says it has contacted Secure Email Cloud customers whose devices showed possible indicators.

SOURCES

Cisco Secure Email Gateway Arbitrary File Write Vulnerability (Cisco PSIRT) - Primary source

CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA - Primary source

CVE-2026-76519 (Mallory vulnerability record) - Reporting / context

04 / THE BRIEF

SiteGuard WAF command injection under active exploitation

BleepingComputer reports CVE-2026-106931, a command injection in the default-on statistics feature of SiteGuard's Server Edition WAF, is being exploited to run commands as root or SYSTEM. SiteGuard's bulletin confirms abuse and JPCERT/CC warns likewise. The vendor says patching may erase attack traces, so pull the diagnostic information first.

QUALIFICATIONS

Single-source so far: everything rests on BleepingComputer quoting the two advisories; neither was read directly.

SOURCES

Hackers exploit SiteGuard WAF flaw to run commands as admins (BleepingComputer) - Reporting / context

05 / THE BRIEF

Some Rank Math SEO PRO downloads carried malware for eleven hours

Some Rank Math SEO PRO 3.0.123 packages downloaded or auto-updated in an eleven-hour window - 20:02 UTC on 15 October to 07:12 on the 16th - carried malware that recreates hidden backdoors on page visits, phones home to rank1cdn[.]com and exposes every secret the web server can reach. Clean 3.0.124 is out and the bug is CVE-2026-111862, 9.8. The version alone doesn't damn you (only packages from that window, which Rank Math says it can identify), but an activated copy means treating the site as compromised - updating doesn't evict anything already planted.

QUALIFICATIONS

Wordfence's own page was erroring when checked, so details come via a full repost, and affected download numbers aren't public.

SOURCES

Supply-Chain Compromise Injects Malware into Some Rank Math SEO PRO Downloads - Reporting / context

PSA: Malware Found in Some Rank Math SEO PRO 3.0.123 Downloads (malware.news, full repost of the Wordfence PSA) - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.