



What small and mid-size business leaders need to know about cyber risk this week, in one page.

Provided by Major Business Solutions LLC

HEADLINE THREAT

ACTIVE EXPLOITATION · CISA DEADLINE OCT 19

Hackers are breaking into remote-support and VPN tools. BeyondTrust is the most urgent fix.

On October 16, CISA added a critical flaw in **BeyondTrust Remote Support** (CVE-2026-102764, CVSS 9.3) to its Known Exploited Vulnerabilities list and urged immediate patching plus a forensic review. A China-linked espionage group exploited it as a zero-day from late August. Attackers planted web shells, tried to steal stored credentials, deleted logs, and **used the tool's own remote sessions to reach the computers it manages**. BeyondTrust patched its cloud (SaaS) customers on October 9. Self-hosted appliances need patch BT26-05-RS applied manually.

It is part of a wider pattern this week. CISA also added actively exploited flaws in Ivanti Connect Secure VPN, Palo Alto firewalls, Cisco's email gateway, Ahsay backup servers and Fortinet FortiOS. All of these tools sit at the edge of a network and are trusted by default.

Why it matters for you

Remote-support tools, VPNs and firewalls are the keys to your network. Many SMBs never see these tools directly because an IT provider or MSP runs them. If one is compromised, an attacker can reach every machine it manages at once. According to the 2026 Verizon DBIR, exploited vulnerabilities are now the most common way attackers get in, ahead of stolen passwords.

PATCH PRIORITY

Critical · KEV 10/16 **BeyondTrust Remote Support / PRA (self-hosted)** CVE-2026-102764: Apply BT26-05-RS. Versions older than 24.3.1 must upgrade first. Exploited since August, so check for signs of compromise too.

VPN · KEV 10/13 **Ivanti Connect Secure** CVE-2026-104935: Unauthenticated command execution, exploited as a zero-day. Update to 22.8R2.5 / 25.1.1.2 / 25.1.3.x.

Firewall · KEV 10/14 **Palo Alto PAN-OS** CVE-2026-0322: Code execution in the management interface. Patch it, and allow management access only from trusted internal IPs.

Critical · KEV 10/14 **Cisco Secure Email Gateway** CVE-2026-76519: A crafted attachment can give attackers root. Upgrade, or update Content Scanner Tools to 25.3.0.5525 or later.

Backup/MSP · KEV 10/14 **Ahsay AhsayCBS** CVE-2026-105133 / -105134: These two flaws are chained to plant web shells. Earlier fixes were incomplete. Install v10.3.4.45 or v9.15.2.70.

Firewall · KEV **Fortinet FortiOS** CVE-2025-61624: Being used to install the stealthy PEERSTITCH implant. Confirm you are on the April 2026 fix or later.

Windows · Zero-day **Microsoft Windows Shell** CVE-2026-96951: A Mark-of-the-Web bypass that helps malicious downloads skip warnings. Fixed in October Patch Tuesday.

BY THE NUMBERS

31%

of breaches began with an exploited vulnerability, now the top way in
Verizon DBIR 2026

48%

of breaches involved a third party, such as a vendor or service provider
Verizon DBIR 2026

48%

of breaches involved ransomware
Verizon DBIR 2026

\$3.05B

lost to business email compromise in 2025 (24,768 complaints)
FBI IC3 2025 Report

THREE ACTIONS THIS WEEK

1. **Get a written answer from IT or your MSP by Monday.** Ask: "Do we, or do you on our behalf, run BeyondTrust, Ivanti, Palo Alto, Fortinet, Cisco email gateway or Ahsay? Are they patched to this week's fixes, and are their admin pages blocked from the internet?"
2. **Patching is not enough. Ask for a compromise check.** Self-hosted BeyondTrust and Ivanti VPNs were exploited before patches existed, and updating does not remove an attacker who is already inside. Also, if anyone uses *AOMEI Backupper* or *AnyViewer*, have IT hunt for that vendor's tampered-update backdoor (May–July 2026).
3. **Finish October Windows updates and retire unsupported PCs.** Make sure every PC has the October 13 updates installed. Windows 11 24H2 Home and Pro got their *last* security update this month, so plan to upgrade those machines now.



Provided by Major Business Solutions LLC

Sources

1. [The Hacker News: China-linked hackers exploited BeyondTrust zero-day \(Oct 16, 2026\)](#)
2. [CISA: Adds Two Known Exploited Vulnerabilities to Catalog \(Oct 13, 2026\)](#)
3. [CISA: Adds Four Known Exploited Vulnerabilities to Catalog \(Oct 14, 2026\)](#)
4. [CISA: Known Exploited Vulnerabilities Catalog](#)
5. [Rapid7: Ivanti Connect Secure zero-day exploited in the wild \(Oct 13, 2026\)](#)
6. [Help Net Security: CISA flags exploited flaws in Palo Alto, Cisco and Ahsay products \(Oct 15, 2026\)](#)
7. [BleepingComputer: Cisco patches Secure Email Gateway zero-day exploited in attacks](#)
8. [The Hacker News: PEERSTITCH malware deployed via FortiOS flaw \(Oct 16, 2026\)](#)
9. [The Hacker News: Attackers tampered with AOMEI Backupper's update servers \(Oct 16, 2026\)](#)
10. [BleepingComputer: Microsoft October 2026 Patch Tuesday fixes 3 zero-days \(Oct 13, 2026\)](#)
11. [Verizon: 2026 Data Breach Investigations Report, Executive Summary](#)
12. [FBI IC3: 2025 Internet Crime Report](#)

Always verify advisories and patch details directly with CISA (cisa.gov) and your vendors before acting. This briefing is a summary, not a substitute for vendor guidance.