



One page. The threat that matters most this week, and what to do about it.

Provided by Major Business Solutions LLC

---

## HEADLINE THREAT

ACTIVE EXPLOITATION · CISA KEV

### Ivanti Connect Secure VPN zero-day (CVE-2026-104935) being used to break into networks

On October 13, Ivanti disclosed that attackers had been exploiting an authentication-bypass flaw (CVSS 8.6) in its Connect Secure VPN appliance before a fix existed. The attacker needs no password and can run commands on the device. CISA added it to the Known Exploited Vulnerabilities (KEV) catalog the same day. Volexity, which found the activity in early October, says the attackers chained it with two more flaws. One of those is **still unpatched**. The intruders stole credentials, exfiltrated data, tampered with logs and mapped internal networks. This is the sixth Ivanti flaw CISA has added to KEV in 2026.

It's part of a busy week for exploited "front-door" devices. CISA also flagged exploited flaws in Palo Alto Networks firewalls, Cisco's email security gateway, and the Ahsay backup console used by many managed service providers (MSPs). Microsoft's record-breaking October Patch Tuesday (more than 1,400 CVEs) includes a Windows flaw that is already being exploited.

**Why it matters for you:** Your VPN and firewall are the doors to your business. They sit on the internet around the clock, and attackers now break in through unpatched software more often than through stolen passwords. If you or your IT provider run Ivanti Connect Secure, patching alone isn't enough. Assume a device that was exposed in early October could already be compromised, and check it.

## PATCH PRIORITY

**PATCH NOW** **VPN** **Ivanti Connect Secure, CVE-2026-104935.** Upgrade to 22.8R2.5, 25.1.1.2, or 25.1.3.0/25.1.3.1. A related privilege-escalation bug is still unfixed. Check for signs of compromise and reset VPN credentials.

**FIREWALL** **Palo Alto Networks PAN-OS, CVE-2026-0322** (CVSS 8.6). An attacker who can log in to the management interface can run code as root. Fixes cover 10.2 through 12.2. Restrict the management interface to trusted internal IPs.

**WINDOWS** **Microsoft Windows Shell, CVE-2026-96951** (CVSS 8.8). A Mark-of-the-Web bypass, exploited in the wild, that lets malicious attachments and downloads skip security warnings. Fixed in the October 13 updates.

---

**EMAIL Cisco Secure Email Gateway, CVE-2026-76519** (CVSS 9.8). A crafted attachment gives the attacker root access. Upgrade AsyncOS to 16.5.0-780 or install Content Scanner Tools 25.3.0.5525 or later.

---

**MSP / BACKUP Ahsay AhsayCBS, CVE-2026-105133 & CVE-2026-105134.** Attackers chain an authentication bypass with a SYSTEM-level command injection to plant webshells and cryptominers. Earlier hotfixes were incomplete. Install 10.3.4.45 (v10) or 9.15.2.70 (v7–9), then reboot.

## BY THE NUMBERS

**\$20.9B**

US cybercrime losses reported to FBI IC3 in 2025, up 26% from 2024

**\$3.05B**

Business email compromise losses in 2025 (24,768 complaints), per FBI IC3

**#1**

Exploited software flaws are now the top way attackers get in, ahead of stolen credentials (Verizon DBIR 2026)

**48%**

Share of breaches involving a third party or supplier, up from 30% the year before (Verizon DBIR 2026)

## THREE ACTIONS THIS WEEK

1. **Patch the front door today.** Ask whoever manages your network: "Do we run Ivanti, Palo Alto or Cisco email security, and is it on this week's fixed version?" Get the answer in writing. If you run Ivanti Connect Secure, also check the device for signs of compromise and reset VPN passwords.
2. **Push October's Windows updates to every PC this week, not next month.** The exploited Windows Shell flaw lets booby-trapped attachments skip security warnings. Remind staff not to open unexpected files, even from known contacts.
3. **Check your IT provider's tools.** Nearly half of breaches now involve a third party. Ask your MSP whether it uses AhsayCBS (or any other remote-management or backup console) for your data, and confirm it's patched and not exposed to the internet.

---

 Provided by Major Business Solutions LLC

## Sources

1. [CISA: Adds Two Known Exploited Vulnerabilities to Catalog \(Oct 13, 2026\)](#)
2. [CISA: Adds Four Known Exploited Vulnerabilities to Catalog \(Oct 14, 2026\)](#)
3. [CISA: Known Exploited Vulnerabilities Catalog](#)
4. [Rapid7: Ivanti Connect Secure zero-day exploited in the wild \(CVE-2026-104935\)](#)
5. [BleepingComputer: Ivanti warns of Connect Secure zero-day exploited in attacks](#)
6. [The Record: New Ivanti and Microsoft bugs under exploitation \(Oct 14, 2026\)](#)
7. [BleepingComputer: Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days](#)
8. [Redmond Magazine: Microsoft October Patch Tuesday sets another record](#)
9. [Help Net Security: CISA flags exploited flaws in Palo Alto, Cisco and Ahsay products \(Oct 15, 2026\)](#)
10. [BleepingComputer: Unpatched AhsayCBS flaws exploited to deploy webshells, mine crypto](#)
1. [McDonald Hopkins: summary of FBI IC3 2025 Internet Crime Report \(Apr 2026\)](#)
2. [Cyber Readiness Institute: summary of Verizon 2026 DBIR findings for small businesses](#)

Statistics come from the FBI IC3 2025 Internet Crime Report (published April 2026) and the Verizon 2026 DBIR, as summarized by the linked sources. Always verify advisories and patch versions directly with CISA ([cisa.gov](https://cisa.gov)) and your vendor before acting.