

This Week's Critical Vulnerabilities: What Executives Should Know and Ask

Disclosures October 13–22, 2026 | Most involve active or attempted exploitation

BOTTOM LINE. Six significant vulnerability disclosures landed in ten days, several of them already used by attackers before or at disclosure. Each one tests whether a company can quickly answer: **Are we exposed? Are we fixed? Were we already breached?** A company that cannot answer within a few business days has a program gap that will resurface with the next disclosure.

WHAT HAPPENED

Issue	What it means in plain English	Status (as of Oct 22)
PHP2Shell CVE-2026-109618 / -109619 CVSS 9.2 First reported Oct 20	PHP is the software that runs most websites, including WordPress sites and many online stores. These flaws let a stranger take control of a company's web server without a password. Instructions for the attack leaked before the fix was ready, and PHP is also hidden inside many products companies buy.	Fixed Oct 21; versions 8.1 and older get no fix. FBI and CERT-EU alerts issued. Exploitation attempts reported by security firms.
BeyondTrust Remote Support CVE-2026-102764 CVSS 9.3 First reported Oct 15	IT help desks use this tool to take over employees' computers from afar to fix problems. Hackers linked to China used a flaw in it to quietly get inside companies for about seven weeks before anyone was warned.	Exploited since late Aug; on CISA's exploited list Oct 16. Cloud version auto-patched; self-hosted installs must be patched manually.
Network "front doors" Ivanti VPN, Palo Alto firewalls, Cisco email gateway First reported Oct 13–14	The equipment that guards the company's front door, such as the system employees use to log in from home, firewalls and email filters, had flaws that let attackers walk right through. In the Ivanti case, even fully updated devices were taken over.	Attackers have already used all three flaws in real attacks, not just in lab tests. CISA urged immediate patching (Oct 13–14).
eMudhra certificate authority 8 compromised signing keys First reported Oct 17	Companies like eMudhra vouch that a website is real; that is what the padlock in your browser means. eMudhra made eight of its vouching keys so carelessly that anyone could copy them, letting criminals build convincing fake websites, listen in on private connections, or make malware look like trusted software.	Blocked by browsers Oct 17–20 and revoked. Apps with built-in trust lists may still accept them. Exposed since April 2025; no misuse seen.
PwnEscape (Linux) CVE-2026-99999 CVSS 9.3 First reported Oct 15	Cloud providers run many customers on the same physical computer. An 18-year-old flaw lets one customer peek into that shared computer's memory, crash it, or, in lab tests, take it over, putting the customers next door at risk. It matters mostly through the cloud and software providers you rely on.	Fix requires a patched host kernel and reboot. No confirmed exploitation as of Oct 21.
LiteLLM AI gateway Malicious release v1.107.0 First reported Oct 21	LiteLLM is a popular free tool, downloaded about 23 million times a week, that connects company software to AI services. Using stolen developer passwords, attackers slipped password-stealing malware into an official update. Anyone who installed it may have handed over the keys to their cloud and AI accounts.	The infected update was available to download for about two hours on Oct 21 before it was pulled. Anyone who installed it must rebuild and change exposed passwords and keys. Second compromise of this tool in 2026.

WHAT EXECUTIVES SHOULD BE ASKING TO LIMIT THE NEXT INCIDENT

Area	Questions leadership should be able to answer	NIST CSF 2.0
Exposure visibility	Within a day, could we list every system the public can reach and every product that contains the affected software, including ones our vendors run for us?	ID.AM, ID.RA
Patch speed for exploited flaws	When attackers are already using a flaw, how fast do we actually fix it on equipment that faces the internet? Can we make emergency fixes without waiting for scheduled maintenance?	PR.PS, ID.RA
Assume-breach verification	After we fix a flaw, who checks whether attackers already got in? Do we keep activity records long enough to look back two months or more?	DE.CM, DE.AE, RS.AN
Privileged and remote access	Which tools and accounts have the power to take over our systems? Are they hidden from the public internet, protected by more than a password, and watched?	PR.AA, PR.IR
Third-party assurance	Can the outside companies that run our systems and software tell us within three days whether they were affected and when they fixed it? Do our contracts require it?	GV.SC
AI and developer tooling	Do we know which AI tools and free software building blocks our teams and vendors use? If one is hacked, could we change every password and access key it holds within hours?	ID.AM, GV.SC, PR.AA
Governance and disclosure	Who decides whether an incident is serious enough that we must disclose it? Do we know every deadline to notify regulators (such as the SEC), customers and our insurer? Does the board see how fast we find and fix problems?	GV.OV, RS.CO

KEY RISK THEMES ACROSS THE ENTERPRISE

Perimeter and remote access. Security and remote-access products are now a favorite way in, and are often left unmonitored.

Third-party and cloud concentration. One breached provider can expose many customers at once; this week, one exposed settings for 500+ firewalls.

Identity and privileged access. Tools and accounts that hold the keys give attackers trusted access once compromised.

Silent exposure windows. Attacks can start long before anyone is warned, as with BeyondTrust. Patched does not mean clean.

Hidden and inherited software. Vulnerable software hides inside vendor products. You cannot fix what you do not know you run.

AI tooling and software supply chain. AI tools hold keys to cloud and AI accounts. One poisoned update can hand them to attackers.

HOW CROSSCOUNTRY CONSULTING CAN HELP

Near term

- Portfolio exposure triage across internal and vendor-supplied systems
- Independent patch verification
- Compromise assessment coordination
- Vendor outreach
- A standard portfolio attestation template

Longer term

- NIST CSF 2.0 assessment of vulnerability management and asset inventory
- Privileged and non-human identity review
- AI tooling and software supply chain governance
- Third-party risk program uplift
- SEC cyber disclosure readiness

REMEDIATION ACTIONS BY ISSUE (TECHNICAL)

Issue	Fix now	Then verify and contain
PHP2Shell CVE-2026-109618 CVE-2026-109619	• Update to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or the fixed package from your Linux or hosting vendor. Internet-facing sites first; Apache mod_php is the highest risk. • Reboot the server (or at least restart PHP and the web server). Running PHP workers keep the vulnerable code until restarted. • PHP 8.1 and older: no fix exists. Upgrade, isolate, or take offline, as the NSA advises for any system that cannot be updated now.	• Confirm the running PHP version on each server, not just the installed package. • Hunt for PHP processes launching command shells or downloading files. • Ask vendors whose appliances or hosted sites bundle PHP when they patched.
BeyondTrust Remote Support CVE-2026-102764	• Self-hosted 24.3.1 to 26.2.3: apply the BT26-05-RS patch in /appliance, or confirm auto-update installed it. • Older than 24.3.1: upgrade to a supported version first, then patch. • SaaS: patched by BeyondTrust by Oct 9; get written confirmation. Patch self-hosted Privileged Remote Access appliances as a precaution.	• Assume breach back to Aug 29: check appliances for web shells, unexpected files, permission changes and deleted logs. • Rotate credentials stored in BeyondTrust and accounts it can reach. • Restrict the admin console from the internet. Ask MSPs and vendors that use BeyondTrust to reach your systems whether they are patched.
Ivanti Connect Secure VPN CVE-2026-104935	• Install the Oct 13 fixed release. Affected: 22.8R2.4, 25.1.1.1 and 25.1.2.2 and earlier. • Third flaw unpatched: the privilege escalation step has no fix yet. Limit who can reach the VPN and watch for Ivanti's next release.	• Forensic review: Ivanti's Integrity Checker may miss this attack because it runs in memory. • Rotate domain credentials, local admin (LAPS) passwords and BitLocker recovery keys the VPN could reach; attackers targeted all three.
Palo Alto PAN-OS firewalls CVE-2026-0322	• Upgrade to the fixed PAN-OS release for your version (10.2, 11.1, 11.2, 12.1, 12.2). • Remove the management interface from the internet; allow only trusted admin addresses.	• Rotate firewall admin passwords and require MFA; exploitation needs an admin login. • Review admin login and configuration-change logs for activity you cannot explain.
Cisco Secure Email Gateway CVE-2026-76519	• Upgrade to AsyncOS 15.5.5-014 or 16.5.0-780 (or Content Scanner Tools 25.3.0.5525+). No workaround exists. Cloud gateway customers need no action.	• Check logs outside the device (network and firewall), since attackers with root can hide evidence. Look for unexpected uploads to external addresses. • Clusters: replace SSH keys shared between appliances, which root access may expose.
eMudhra certificate authority 8 compromised signing keys	• Replace any of your certificates issued by eMudhra (emSign) with ones from another authority before Chrome drops its root on Oct 27. • Update software that carries its own trust list: Go 1.27.3 / 1.26.10 (then rebuild apps), Node.js 22.23.4 / 24.22.1 / 26.12.1, Python certifi 2026.10.19, NSS 3.131.1, Firefox 158.0.1.	• Ask vendors whether their appliances, agents and SaaS rely on built-in trust lists and have updated them. • Code signing: two of the keys signed software. Block anything signed with them and check TLS-inspection proxies and internal trust stores.
PwnEscape (Linux) CVE-2026-99999	• Update Linux hosts that run virtual machines or containers to the latest stable kernel with the fix, then reboot. • Prioritize hosts running workloads you do not control: shared hosting, CI runners, sandboxes.	• Ask cloud, hosting and SaaS providers when their hosts were patched and rebooted. • Watch for unexplained host crashes tied to virtual machine network traffic.
LiteLLM AI gateway Malicious v1.107.0	• Find any system that installed 1.107.0 from PyPI or ran Docker tags v1.107.0, latest, main-latest or main-stable on Oct 21. • Isolate and rebuild from a clean image on 1.106.2. Uninstalling is not enough; the malware runs on every Python start.	• Rotate every credential the host could reach: cloud and SSH keys, CI/CD secrets, AI provider keys, the LiteLLM master key and stored provider keys, browser passwords. • Review cloud and AI provider logs for misuse; abuse of stolen keys was seen within hours. Block the lookalike domain litellm[.]dev.

Contact: Adel Zahiry, Partner, Cybersecurity & Privacy | azahiry@crosscountry-consulting.com

Sources: PHP Security Advisory; NSA PHP advisory; FBI, CERT-EU and CISA alerts and KEV updates (Oct 13–21); BeyondTrust BT26-05; Ivanti, Palo Alto Networks and Cisco advisories; Volatility analysis; Mozilla incident report, Chrome Root Program and eMudhra statement; LiteLLM incident report and OpenSSF MAL-2026-2144; Linux CVE-2026-99999 record. Current as of Oct 22, 2026; check CISA KEV for updates. General guidance only; not legal advice on notification obligations.