

— SECURITY / 3 MIN READ

Change the locks today

On 21 October a hosting platform told its users to change every secret, a popular AI package shipped a password stealer, and PHP rushed out fixes for flaws attackers were already probing.

WHAT HAPPENED

01 PHP2Shell

Two flaws in PHP let anyone run their own code on an unpatched server, no login needed. Details leaked on 20 October and fixes shipped the next day. Amazon logged a first attempt on the 17th, and broad attempts followed. Releases back to 5.4 are affected. Official fixes cover 8.2 and up; 7.4 to 8.1 get backports.

02 Railway

Railway, a platform developers use to deploy apps, said an intruder may have read customers' stored secrets, such as API keys and database passwords. It told users to change them. Deployments resumed on 22 October, and on 24 October OpenAI and Anthropic revoked some freshly rotated keys as a precaution.

03 Poisoned AI developer packages

LiteLLM 1.107.0, a popular package for calling AI models, went out through its own engineers' GitHub accounts carrying a credential stealer and a backdoor. It runs as soon as Python starts. Earlier this month tensorlake 0.5.144 on npm stole keys too, and wipes the home folder if its GitHub token is revoked.

04 Certificate keys and the edge

Eight eMudhra certificate-authority keys could be guessed, so a fake site or signed program could pass as genuine. Browsers and operating systems now block them. Separately, a suspected Chinese espionage group has used a BeyondTrust remote-support flaw since late August, and firewalls, VPNs and email gateways are under attack.

THE NEXT 72 HOURS, MOST URGENT FIRST

Name one owner to work this list and report to the CEO daily.

- 01 Patch the front door and the app.** Apply this month's fixes to remote-support tools, VPNs, firewalls, email gateways and self-managed GitLab, including Fortinet's 22 October updates before their details go public on 10 November. Update Next.js to 16.4.1 or 15.5.28, and Node.js to 22.23.4, 24.22.1 or 26.12.1 for a Brotli flaw (CVE-2026-111497). Treat a BeyondTrust appliance left exposed and unpatched as broken into until it is checked, and keep management interfaces off the open internet.
- 02 On Railway? Change every secret stored there,** registry passwords included, then check the logs of whatever those secrets unlock. If a provider revoked a new key, issue another and redeploy.
- 03 Hunt for the bad packages.** Search laptops, servers, containers and build jobs for LiteLLM 1.107.0, from PyPI or Docker, and tensorlake 0.5.144, and for `.claude` or `.vscode` files nobody wrote. If you find one, wipe that machine first, then change every key it could reach from a clean one. Pin LiteLLM to 1.106.2.
- 04 Patch PHP.** A WordPress site runs on PHP. Ask your engineers and web host where else it runs, and on which version. Update to 8.2.35, 8.3.36, 8.4.27 or 8.5.12 today. On 7.4 to 8.1, apply the backport; anything older must be upgraded. Have any server exposed since 17 October checked for a break-in.
- 05 Ask your vendors, in writing,** whether they have patched PHP2Shell and whether they run on Railway or reach your systems through BeyondTrust. Keep the replies.
- 06 Update every device.** Normal updates carry the eMudhra blocks, so turn them on wherever they are off; servers and apps need fresh certificate stores too. Chrome removes the emSign ECC Root CA - G3 on 27 October, so any site with a certificate from it needs a new one.

WITHIN 30 DAYS

01

Keep a current list of your systems and the software inside them, so the next "do we run this?" takes minutes.

02

Map your blast radius. If one server fell, what else could an attacker reach? Cut access no one needs.

03

Hold new releases of developer packages for a few days. Keep keys in a vault, never in code.

04

Write down who decides in an incident and who they call. Keep logs long enough to look back a month.



Nonlinear Advisors
Steady hands for nonlinear growth.

Need a hand? Our security team can check where you stand within days.

info@nonlinearadvisors.com | nonlinearadvisors.com | [LinkedIn](#) | [X](#)

Based on public reporting as of 26 October 2026 from the PHP project, Railway, LiteLLM, Amazon, Cloudflare, CISA, Google, Mandiant, BeyondTrust, GitLab, Vercel, Node.js, Fortinet, The Hacker News and BleepingComputer; details are still changing. Nothing in this advisory is legal, tax or investment advice. © 2026 Nonlinear Advisors LLC, New York.