

Has your website been patched?

A plain-English guide for website owners on the PHP2Shell alert

Version 1.0 · **Published:** October 23, 2026, 7:00 AM ET · **Last verified:** October 22, 2026, 11:20 PM ET ·
For: website owners and business teams. This is not a server administration runbook.

You don't need to understand PHP to ask whether your website is affected. This guide gives you the message to send, explains the answers you might get back, and helps you follow up without becoming a server administrator.

Your next step: forward the Patch Question below to whoever maintains your website today.

This is a dated edition. Check the guide's web page at getaiminute.com/guides/php2shell-website-owner for updates before relying on the technical details.

Current advisory (verified October 22, 2026, 11:20 PM ET)

- **What:** two critical flaws in PHP, CVE-2026-109618 and CVE-2026-109619, known as PHP2Shell. The PHP project says they "can allow unauthenticated remote code execution." [PHP](#)
- **Fixed in:** PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35, released October 21, or a vendor package that contains both fixes. PHP has also supplied limited source patches for 7.4, 8.0 and 8.1, which no longer get regular releases.
- **Attacks:** Amazon, Cloudflare and watchTowr report attack activity. How many systems have been broken into is still unclear. [Tenable watchTowr](#)
- **Official guidance:** the FBI says that if an immediate update isn't feasible, "take the system offline until it can be fully mitigated." [FBI Cyber Division](#)

1. Start here: who runs your website?

The answer comes from whoever maintains the software behind your site. That's usually one of these:

- your web hosting provider;
- the agency or freelancer who built or maintains the site;
- your company's IT team;
- the vendor behind a business application you log into.

Not sure who? Send this to whoever you do know:

Who maintains the server software behind our website? Please pass this to the person who can confirm whether both PHP2Shell fixes (CVE-2026-109618 and CVE-2026-109619) have been applied.

2. The Patch Question

Copy this and send it. It's the same message as in our bulletin.

```
Subject: PHP2Shell: please confirm our patch status
```

```
Do any of our websites or business tools run PHP? If yes, please confirm:
```

- ```
1. Have both CVE-2026-109618 and CVE-2026-109619 been fixed? Which PHP version or vendor-patched package is running, and when was it applied?
2. Have the PHP workers been restarted and the running version verified? Is anything still on PHP 8.1 or older?
3. Have logs and server activity been reviewed from at least October 17 for signs of exploitation?
4. If anything can't be patched right away, is it being taken offline until it can be fully mitigated, as the FBI recommends?
```

---

## 3. What does their answer mean?

You aren't certifying anything yourself. You're getting a clear answer from the people responsible.

| What they say            | What to ask next                                                                                     |
|--------------------------|------------------------------------------------------------------------------------------------------|
| "You're not affected."   | "Thanks. Can you tell us what you checked, and why these flaws don't apply?"                         |
| "We patched it."         | "Which version or vendor package is running now, and when did you verify it?"                        |
| "Our host handles that." | "Can you get written confirmation from the host and send it to us?"                                  |
| "We use Cloudflare."     | "Understood. Have both fixes also been applied to the PHP installation underneath?"                  |
| "We're looking into it." | "Who owns this, what's the system's status right now, and when will we hear next?"                   |
| "We can't update yet."   | "What's stopping the update, and is the system being taken offline until it can be fully mitigated?" |

A firewall rule can reduce exposure. It doesn't replace the update. The PHP team says its temporary workarounds "do not make an installation safe." [PHP](#)

---

## 4. The three answers you want

Every reply should end up in one of these:

- **Not affected:** your provider checked and explained why the flaws don't apply. Keep that explanation.

- **Fixed:** both fixes are applied, running and verified. Keep the version, the date and how they checked.
- **Not yet fixed:** keep a record of who owns the response, whether the system is offline, and when the next update is due.

A pending support ticket is not the same as a confirmed fix.

Two things need separate answers: whether the fixes are running, and whether your provider's review found signs of exploitation. Ask for confirmation of both.

---

## 5. If your provider suspects a break-in

This is the point to bring in whoever handles security incidents for your organization. Don't treat the rest of this guide as a do-it-yourself recovery plan.

The FBI's advice: isolate the affected systems, keep the web server and PHP logs, and report it to your local FBI field office or [ic3.gov](https://ic3.gov). [FBI Cyber Division](#)

---

## 6. Keep a record

Useful if you look after more than one site, or need to show your manager or a client what was done.

| Item                                                       | Your record |
|------------------------------------------------------------|-------------|
| Website or application                                     |             |
| Who maintains it                                           |             |
| Contact or ticket number                                   |             |
| Status: not affected, fixed or not yet fixed               |             |
| Exploitation review: pending, no signs found, or escalated |             |
| Fix or explanation they gave                               |             |
| Date and time verified                                     |             |
| Next update due                                            |             |

---

*Version 1.0, a dated edition. Check [getaiminute.com/guides/php2shell-website-owner](https://getaiminute.com/guides/php2shell-website-owner) for updates. From The AI Minute. We read 47 AI and tech newsletters so you don't have to. Editorial guidance only; this isn't a security audit or legal advice. Get the weekly brief free at [getaiminute.com](https://getaiminute.com).*