CHECKLIST · SCAMS & SECURITY

PHP's critical fixes are out. Has your website been patched?

Published 22 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/php2shell-fixes-released-what-to-check/

- [ ] **Ask your host or developer whether PHP has been updated.** Your site should be on 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or a patched build from your host.
- [ ] **Don't rely on WordPress or plugin updates for this.** WordPress says none is required or planned; the fix is a PHP update on the server.
- [ ] **Ask what your host is doing for PHP 8.1 or older.** PHP's regular releases skip them, and the only fixes for 7.4 to 8.1 are source code for people who build PHP themselves.
- [ ] **Plan a move off PHP 8.2 before 31 December.** That's when PHP stops releasing security fixes for it.
- [ ] **Use an HTTP 503 status if you take the site offline.** Ask your developer to set it, through your DNS or CDN provider if PHP is down, and keep the outage to a few days at most.
- [ ] **Contact the ACSC if you think your site has been attacked.** Call 1300 CYBER1 (1300 292 371).

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.