

PHP2Shell

Sicherheitslücke in PHP („PHP2Shell“): Was Sie jetzt wissen sollten

Kurz zusammengefasst

In der weit verbreiteten Programmiersprache PHP wurden zwei kritische Sicherheitslücken entdeckt. Sie tragen den Namen „**PHP2Shell**“ und die Kennungen **CVE-2026-109618** und **CVE-2026-109619**. Beide Lücken werden mit 9,2 von 10 Punkten bewertet.

Ein Angreifer kann die Lücken über das Internet ausnutzen, **ohne sich anzumelden**, und dabei eigenen Programmcode auf einem betroffenen Server ausführen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Lücke mit der Warnstufe **Orange** ein und hält schnelle Angriffe für wahrscheinlich.

Die gute Nachricht: Die PHP-Entwickler haben am 21.10.2026 korrigierte Versionen ab PHP 8.2 veröffentlicht.

Prüfen Sie den Einsatz von PHP und führen Sie die Updates sofort durch.

Was ist PHP?

PHP ist eine Software, die im Hintergrund vieler Webseiten, Online-Shops und Kundenportale arbeitet. Auch bekannte Systeme wie WordPress, Joomla, TYPO3, Shopware, Magento, Nextcloud, Roundcube oder phpMyAdmin nutzen PHP. Die Lücke betrifft daher nicht ein einzelnes Programm, sondern die Grundlage, auf der diese Programme laufen.

Bin ich betroffen?

Sie sind **wahrscheinlich betroffen, wenn auf einem Server PHP läuft**, der nicht auf dem neuesten Stand ist. Typische Fälle sind:

- Eigene Webseiten oder Online-Shops, auch bei einem Hoster oder einer Agentur
- Kundenportale und Webanwendungen
- Installationen von Programmen wie WordPress, Shopware oder Nextcloud auf einem eigenen Server
- Geräte oder Programme anderer Hersteller, die intern eine Weboberfläche mit PHP bereitstellen

Normalerweise nicht betroffen sind:

- Normale Windows-PCs und Notebooks
- Microsoft 365 und Outlook
- PHP-freie Anwendungen

Auf einem PC ist PHP nur vorhanden, wenn es gezielt installiert wurde, zum Beispiel für Softwareentwicklung (etwa mit XAMPP).

Was sollten Sie tun?

Schritt	Was genau zu tun ist
1. Prüfen	Ermitteln Sie, welche PHP-Version auf Ihrem Server läuft. Bei gehosteten Webseiten fragen Sie Ihre Agentur oder Ihren Hoster.
2. Aktualisieren	Installieren Sie eine der korrigierten Versionen: PHP 8.5.12, 8.4.27, 8.3.36 oder 8.2.35 (bzw. die von Ihrem Betriebssystem oder Hoster bereitgestellte gepatchte Version).
3. Neu starten	Nach dem Update sollten PHP-Dienste bzw. der Webserver neu gestartet werden, damit die neue Version aktiv wird.
4. Kontrollieren	Lassen Sie sich von Ihrem Betreuer bestätigen, dass das Update eingespielt ist.

Wichtig:

- Ein wirksamer Workaround ist laut BSI derzeit nicht bekannt. Das Update ist die einzige vollständige Lösung.

- Wenn Sie nicht sofort aktualisieren können, sollten Sie betroffene Systeme nach Möglichkeit vom Netz nehmen, bis das Update eingespielt ist.
- **Ältere PHP-Versionen** (z. B. 7.4, 8.0 oder 8.1) erhalten keine regulären Updates mehr. Für sie gibt es nur eingeschränkte Korrekturen. Hier ist der Umstieg auf eine aktuelle PHP-Version die sicherste Lösung.
- Wenn Sie einen Hoster nutzen, prüfen Sie, ob dieser das Update bereits eingespielt hat. Viele Hosters aktualisieren PHP selbst, bei manchen muss die Version im Kundenbereich ausgewählt werden.

Hinweise für Nutzer von Webseiten und Online-Shops

Webseiten und Shops werden oft von einer Agentur oder einem Hoster betreut. Fragen Sie dort gezielt nach dem Stand der PHP-Updates. Das Update selbst sollte von der Person oder Firma durchgeführt werden, die für das System verantwortlich ist.

Gibt es Anzeichen für einen Angriff?

Achten Sie auf Ungewöhnliches, zum Beispiel:

- veränderte Webseiten oder unbekannte Inhalte
- unbekannte Benutzerkonten
- E-Mails, die in Ihrem Namen versendet wurden, ohne dass Sie etwas veranlasst haben

Wenn Sie solche Auffälligkeiten bemerken, handeln Sie zügig: Löschen Sie nichts, starten Sie betroffene Systeme nicht neu und wenden Sie sich umgehend an Ihren Ansprechpartner bzw. an Ihren Betreuer. Eine Sicherheitslücke allein ist noch kein Datenschutzvorfall. Ob ein solcher vorliegt, lässt sich nur im Einzelfall beurteilen.

Unsere Unterstützung

Wir unterstützen Sie gerne bei der Einschätzung Ihrer Systeme. Bei Systemen, die wir für Sie betreuen, prüfen wir den Stand. Für Bereiche, die wir nicht betreuen, bitten wir Sie um Ihre Mithilfe und stellen Ihnen auf Wunsch einen kurzen Fragebogen zur Verfügung. Die Auswertung und eine erste Einschätzung sind für Sie kostenlos. Falls darüber hinaus Arbeiten nötig sind, erhalten Sie

vorher ein Angebot.

Bei Fragen erreichen Sie uns über das [Taskleisten-Symbol](#), telefonisch oder per E-Mail.

Quellen

- PHP-Sicherheitsmitteilung und Versionen 8.5.12, 8.4.27, 8.3.36, 8.2.35 (veröffentlicht am 21.10.2026)
- Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherheitshinweis vom 21.10.2026

Version #9

Erstellt: 2026-10-22 12:04:43 UTC von Marvin Meißner

Zuletzt aktualisiert: 2026-10-22 12:35:01 UTC von Marvin Meißner