



Pressemitteilung

Schwerin, den 22. Oktober 2026

Millionen Webseiten durch kritische Sicherheitslücke potentiell gefährdet – LfDI MV rät zum sofortigen Handeln

Webseiten, Onlineshops, Portale und Webpräsenzen von Behörden rücken ins Visier von Cyberattacken. Schwachstellen in der Webskriptsprache PHP ermöglichen Angriffe auf entsprechende Webserver. Angreifer können nach erfolgreichen Attacken auf Daten zugreifen, diese verändern oder Schadsoftware einschleusen. Systeme müssen deshalb umgehend überprüft und Patches sofort eingespielt werden, um Datenschutzverletzungen zu vermeiden.

Zwei neu veröffentlichte Sicherheitslücken in der Webskriptsprache PHP sorgen derzeit weltweit für erhöhte Aufmerksamkeit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die Lage in einer Mitteilung vom 21.10.2026¹ als kritisch ein. PHP bildet die technische Grundlage zahlreicher Webseiten, Online-Shops, Kundenportale und Webanwendungen. Auch viel genutzte Content-Management-Systeme (CMS) wie WordPress, Joomla oder Drupal basieren auf PHP. Viele Webseiten wurden weltweit vorsorglich offline genommen, was die Kritikalität unterstreicht. Die Sicherheitslücke war geleakt worden, bevor die Sicherheitsupdates bereitgestellt werden konnten, wodurch das Risiko einer Ausnutzung durch Cyberkriminelle immens gestiegen ist. So könnten Angriffe beispielsweise darin bestehen, dass Kriminelle Webseiten übernehmen und die Inhalte (Texte, Bilder, Töne) darauf verändern. Personenbezogene Daten (z. B. Namen, Adressen, Telefonnummern, Geburtsdaten, E-Mail-Adressen, Passwörter, etc.) könnten gestohlen oder Daten verschlüsselt und für deren Freigabe Lösegeld gefordert werden. Zudem könnten Kriminelle die gekaperten Webseiten auch für weitere Cyberattacken nutzen.

Die Sicherheitsupdates stehen seit 21.10.2026, 16.00 Uhr zur Verfügung² und müssen unverzüglich eingespielt werden.

Mögliche Datenschutzverletzungen – Meldung einer Datenpanne

Wird ein System über die PHP-Schwachstelle erfolgreich angegriffen, liegt eine meldepflichtige Verletzung personenbezogener Daten vor. In diesem Fall müssen Verantwortliche diese Meldung nach Art. 33 DS-GVO binnen 72 Stunden nach Bekanntwerden der Verletzung an die zuständige Datenschutzaufsichtsbehörde übermitteln.

1 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261021_PHP-kritische-Schwachstelle.html

2 <https://www.php.net/archive/2026.php#2026-10-21-5>

Bei einem voraussichtlich hohen Risiko für die betroffenen Personen (Kunden, Kontakte, Nutzende) müssen diese umgehend benachrichtigt werden.

Was jetzt zu tun ist

Betreibende bzw. Verantwortliche einer Webanwendung, z. B. eines Online-Shops, Kundenportals, einer Vereinswebseite oder ähnlicher Angebote, müssen umgehend die verwendete PHP-Version kontrollieren und entsprechend bereitgestellte Patches einspielen. Wird zum Betreiben der Webseite ein externer Dienstleister genutzt, was oft der Fall ist, sollte dieser Sie als Verantwortliche bereits bezüglich der Sicherheitslücke und dem weiteren Vorgehen informiert haben. In jedem Fall muss die PHP-Version auf Webservern und Anwendungen überprüft werden.

Folgende korrigierte PHP-Versionen wurden veröffentlicht:

8.5.12

8.4.27

8.3.36

8.2.35

System auch nach Sicherheits-Updates genau überwachen

Ältere nicht mehr unterstützte PHP-Versionen müssen umgehend ersetzt werden. Verantwortliche müssen sich bei ihren Dienstleistern rückversichern, ob die betroffenen Systeme entsprechend abgesichert wurden. Ein bereits installiertes Update schließt einen früheren Angriff jedoch nicht grundsätzlich aus, da die Sicherheitslücke vor Veröffentlichung der Patches bestand, d. h. Angriffe könnten bereits im Vorfeld erfolgreich gewesen sein.

Daher sollte ein Sicherheits-Monitoring, das ohnehin vorhanden sein muss, aktuell noch engmaschiger erfolgen. Konkret müssen Serverprotokolle, ungewöhnliche Anmeldeversuche, auffällige Prozesse oder unerwartete Datenübertragungen besonders genau untersucht werden.

Achtung: Phishing im Kontext der aktuellen Sicherheitswarnungen

Angreifer nutzen die aktuelle Unsicherheit aufgrund der kritischen PHP-Schwachstelle und der damit einhergehenden umfassenden Sicherheitswarnungen für ihre Zwecke aus. In diesem Zusammenhang sind solche Betrugsversuche besonders glaubwürdig. So könnte beispielsweise in gefälschten E-Mails, die angeblich von Hosting-Anbietern, IT-Dienstleistern, Sicherheitsbehörden oder bei Privatpersonen von Online-Shops oder Portalen stammen, behauptet werden, dass die Empfänger aufgrund der PHP-Schwachstelle sofort handeln müssten.

Diese betrügerischen Forderungen sind in der Regel verbunden mit einem Link, der zur Eingabe der persönlichen Login-Daten veranlassen soll und angeblich der Verifizierung dient oder einen Download für das angebliche Sicherheitsupdate bereithält, hinter der sich dann eine Schadsoftware verbirgt. Möglicherweise nutzen die Angreifer vermeintliche Mitteilungen des BSI, vom CERT oder anderen Sicherheitsbehörden, um die Forderungen authentischer wirken zu lassen.

Woran erkennt man eine vertrauenswürdige Information zum Sicherheitsvorfall?

Eine seriöse Mitteilung enthält in der Regel die konkrete Benennung der IT-Schwachstelle sowie der betroffenen Dienste und beschreibt die durchgeführten Maßnahmen. Sie erläutert zudem, welche weiteren Handlungen erforderlich sind. Da aber bei professionell gestalteten Phishing-Mails die Echtheit schwer zu prüfen ist, rät der LfDI MV dazu, keine Links in etwaigen E-Mails anzuklicken, sondern entsprechende Webseiten immer selbstständig aufzurufen oder im Zweifel direkt über einen unabhängigen Kontaktweg (z. B. Telefonservice) beim zuständigen Anbieter nachzufragen.

Grundsätzliches: Backups für den Ernstfall

Wichtig ist das Vorhalten von Datensicherungen für den Fall eines erfolgreichen Angriffs. Diese müssen aktuell, getrennt aufbewahrt und regelmäßig getestet werden. Backups helfen, Schäden erfolgreicher Angriffe zu begrenzen.

Grundsätzlich gilt hier wieder: ein Sicherheitskonzept reduziert das Risiko von erfolgreichen Angriffen. Dazu gehören regelmäßige Updates, sichere Konfigurationen, ein Zugriffsmanagement, Sicherheitsüberwachung sowie ein Notfallmanagement, in dem klare Notfallprozesse definiert sind. Der BSI-Grundschutz bietet hilfreiche Sicherheitstipps.³

Als Privatpersonen können Sie Ihre Daten bestmöglich durch starke Passwörter und – wenn möglich – mithilfe einer Mehrfaktor-Authentifizierung schützen. Zudem sollten Sie derzeit vermehrt Ihre Onlinekonten auf ungewöhnliche Aktivitäten beobachten. Wenn ein Anbieter über einen Sicherheitsvorfall informiert, sollten die enthaltenden Handlungsempfehlungen beachtet werden. Ein sofortiger Passwortwechsel muss immer erfolgen.

Kontakt:

Tel: 0385 5949437

E-Mail: presse@datenschutz-mv.de

3 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html