Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit

BITS-H Nr. 2026-297981-1012, Version 1.0, 21.10.2026

Kritikalität*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Bitte prüfen Sie selbstständig, für welche Stellen in Ihrer Organisation die hier genannten Informationen relevant sind und leiten Sie das Schreiben entsprechend weiter – sofern die TLP-Einstufung dies zulässt.

Übersicht

Betroffenes Produkt	PHP	**Gefährdung**	Kritische Schwachstelle
Betroffene Versionen	alle PHP-Versionen	**Schutzmaßnahmen**	Patch + Workaround
Behebende Versionen	ausstehend	**CVEs**	• CVE-2026-109618 (9.2) • CVE-2026-109619 (9.2)

Sachverhalt

In einer Vorab-Ankündigung informieren die Entwickler von PHP aktuell über die Veröffentlichung von Details und Patches zu zwei Schwachstellen in der Programmiersprache am 21. Oktober 2026 ab 16 Uhr [PHP26a]. Auch wenn zum aktuellen Zeitpunkt nur wenige Details verfügbar sind, legen die Bewertungen nach CVSS (Common Vulnerability Scoring System; Version 4.0) mit 9.2 von 10 nahe, dass es Angreifern auf Basis von CVE-2026-109618 und CVE-2026-109619 gelingen könnte, aus der Ferne schadhaften Code auf Webservern mit PHP-Anwendungen auszuführen [CEU26].

Weiterhin kann aus den CVSS-Scores abgeleitet werden, dass für eine Ausnutzung weder eine Authentifizierung noch eine Nutzerinteraktion erforderlich sind. Die Schwachstellen werden in aktuellen Berichtserstattungen auch als "PHP2Shell" bezeichnet, um die Ähnlichkeit mit der Schwachstelle "Log4Shell" aufzuzeigen.

* 1 / Grau: Maßnahmen sollten in absehbarer Zeit erwogen werden. Keine wesentlichen Beeinträchtigungen zu erwarten.
2 / Gelb: Maßnahmen müssen zeitnah ergriffen werden. Temporäre Beeinträchtigungen des Regelbetriebs möglich.
3 / Orange: Maßnahmen müssen unverzüglich ergriffen werden. Massive Beeinträchtigung des Regelbetriebs möglich.
4 / Rot: Maßnahmen müssen sofort ergriffen werden. Geschäftskritische Beeinträchtigung möglich.

BSI-IT-Sicherheitshinweis

Zum aktuellen Zeitpunkt sind noch keine bestätigten Ausnutzungen der Schwachstellen bekannt, jedoch gibt es bereits unbestätigte Berichte über existierende Exploits.

Der Patch für die Schwachstelle ist heute 16 Uhr deutscher Zeit (14:00 UTC) angekündigt und sollte unverzüglich zu diesem Zeitpunkt installiert werden.

Betroffene Produkte

Aktuellen Informationen zufolge sind **alle bekannten PHP-Versionen**, zurückgehend bis mindestens PHP 5 **verwundbar**. [CEU26]

Bewertung

PHP ist einer der zentralen Bausteine in Webanwendungen weltweit und der Einsatz daher sehr weit verbreitet. Mit dieser Programmiersprache entwickelter Quellcode findet sich dabei nicht nur in klassischen PHP-Webseiten, sondern auch in einzelnen Komponenten von verschiedenen proprietären Produkten. Beispielweise wurden die Open Source Projekte WordPress, Drupal, TYPO3, Joomla, Magento, Nextcloud, pfSense, OPNsense mit PHP entwickelt.

Mit Kenntnis von Schwachstellen in derartigen weit verbreiteten Programmiersprachen oder Bibliotheken könnte es Angreifern gelingen, massive Angriffskampagnen durchzuführen und IT-Systeme aus den unterschiedlichsten Anwendungsbereichen zu kompromittieren.

Zwar sind zum aktuellen Zeitpunkt noch keine Angriffe mithilfe der beiden Schwachstellen beobachtet worden, allerdings hält das BSI eine kurzfristige breite Ausnutzung innerhalb weniger Stunden nach Erscheinen der Patches für wahrscheinlich. Spätestens seit dem Aufkommen von KI-gestützten Tools zur Exploit-Entwicklung verfügen Akteure über die benötigten Mittel um Patches innerhalb kurzer Zeit zu analysieren und Exploits zu generieren. IT-Sicherheitsverantwortliche sollten daher unverzüglich handeln.

Maßnahmen

Mitigation

Die Entwickler stellen am 21. Oktober um 16 Uhr deutscher Zeit Patches für unterschiedliche PHP-Versionen bereit, die vor Angriffen schützen. Details sollen dem kommenden Advisory entnommen werden, dazu sollte https://www.php.net/archive/2026.php verfolgt werden.

IT-Sicherheitsverantwortliche und Betreiber sollten zu diesem Zeitpunkt umgehend die Patches auf PHP-Webserver einspielen sowie den Patchstatus anhand des Advisories verifizieren bzw. abgleichen (mit *php -v*).

PHP wird üblicherweise über die Paketverwaltung (wie bspw. apt) der jeweiligen Linux-Distribution aktualisiert. Ein Abgleich der installierten Version mit der von der Linux-Distribution bereitgestellten gepatchten (Backport) Version ist daher möglicherweise notwendig. Für die Schwachstelle CVE-2026-109618 sollte ein entsprechendes Advisory bspw. bei Ubuntu [UBU26], Debian [DEB26] sowie RedHat [RH26] unter den angegebenen Quellen veröffentlicht werden.

In Docker Containern betriebene Anwendungen müssen davon unabhängig – sofern PHP verwendet wird – aktualisiert bzw. neu gebaut werden. Für Hersteller kann es außerdem notwendig werden, neue Firmware-Versionen mit gepatchten PHP-Versionen zu veröffentlichen.

Alternativ sollte geprüft werden, ob die Entwickler Workarounds anbieten.

Workarounds

Zum aktuellen Zeitpunkt sind keine Workarounds bekannt, die zuverlässig vor einer Ausnutzung schützen können. Das PHP-Advisory könnte jedoch Maßnahmen enthalten, wie eine Ausnutzung verhindert oder zumindest erschwert werden kann.

Die Verwendung einer Web Application Firewall (WAF) könnte eine Ausnutzung verhindern, sofern entsprechende Detektionsmittel für die beiden Schwachstellen zur Verfügung stehen und angewandt werden.

Alternativ kann eine vorübergehende Trennung des Webservers vom Internet bis zum Einspielen des Patches erwogen werden, um eine Kompromittierung zu verhindern, sollten Patches nicht kurzfristig installiert werden können.

Kompromittierung prüfen

Zum aktuellen Zeitpunkt sind keine Angriffe mithilfe dieser Schwachstellen bekannt. Konkrete Angriffsindikatoren liegen demnach nicht vor. Betreiber sollten exponierte PHP-Webserver verstärkt auf Auffälligkeiten beobachten.

An verschiedenen Stellen im Internet werden zwar bereits angebliche Indicators of Compromise und Hunting Guidances präsentiert. Eine verbindliche Empfehlung dieser kann jedoch erst erfolgen, wenn weitere Details zum Sachverhalt bekannt sind. Bis dahin können IT-Sicherheitsverantwortliche eigenverantwortlich prüfen, ob eine Nutzung dieser Angebote zielführend ist.

Empfehlungen

Organisationen sollten dringend die personellen Kapazitäten bereithalten, um unverzüglich auf die Veröffentlichung reagieren zu können.

Im vorliegenden Sachverhalt wird eine Verwundbarkeit bis mindestens PHP 5 attestiert [CEU26]. Dabei haben alle PHP Versionen vor 8.2 bereits ihr End-of-Life erreicht. Auch PHP 8.2 wird nur noch bis zum Jahresende mit Sicherheitsupdates unterstützt. Betreiber von PHP-Anwendungen auf Basis dieser Versionsstränge sollten daher grundsätzlich auf eine PHP-Version migrieren, die noch unterstützt wird.

Davon unabhängig empfiehlt das BSI, den Zugriff auf Webanwendungen – sofern möglich – restriktiv zu gestalten [BSI23], die in diesem Zusammenhang betriebenen Komponenten umfassend zu härten und durch zusätzliche Schutzmaßnahmen, wie z.B. Web Application Firewalls, ergänzend abzusichern.

Referenzen

[PHP26a] PHP News - Upcoming Critical PHP Security Release
https://www.php.net/archive/2026.php#2026-10-20-1

[UBU26] Ubuntu Advisory - CVE-2026-109618
https://ubuntu.com/security/CVE-2026-109618

[DEB26] Debian Advisory - CVE-2026-109618
https://security-tracker.debian.org/tracker/CVE-2026-109618

[RH26] RedHat Advisory - CVE-2026-109618
https://access.redhat.com/security/cve/CVE-2026-109618

[CEU26] CERT-EU Security Advisory - Critical Vulnerabilities in PHP
https://cert.europa.eu/publications/security-advisories/2026-018/

[BSI13] Leitfaden zur Entwicklung sicherer Webanwendungen:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftragnehmer.pdf

[BSI23] BSI IT-Grundschutz: APP.3.1 Webanwendungen und Webservices (Edition 2023)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_3_1_Webanwendungen_und_Webservices_Edition_2023.html

Versionsverlauf

Version 1.0 — 21.10.2026

Mit den hier veröffentlichten Informationen weist das BSI anlassbezogen auf Sicherheitsrisiken mit herausragendem Bedrohungspotenzial hin. Bitte beachten Sie außerdem die tagesaktuellen Hinweise im WID-Portal auf https://www.cert-bund.de, um IT-Komponenten vor Cyber-Angriffen zu schützen.

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.