

PREPARE PROTECT DETECT RESPOND IMPROVE

● AUSNUTZUNGSVERSUCHE BEOBACHTET · SEIT 17.10.2026

THREAT INTELLIGENCE BRIEFING

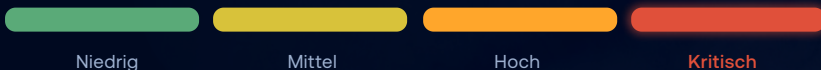
CVE-2026-109618 · CVE-2026-109619

„PHP2Shell“: Code-Ausführung im PHP-Kern ohne Anmeldung.

Zwei Speicherfehler im Kern von PHP erlauben es einem Angreifer aus dem Internet, ohne Anmeldung Code auf dem Webserver auszuführen – teils bevor die eigentliche Anwendung überhaupt startet. Betroffen ist praktisch jede PHP-Installation, die Webanfragen bedient: WordPress, Drupal, Joomla, Magento, Shops und Eigenentwicklungen. Ein CMS-Update hilft nicht, nur ein neues PHP. Erste Ausnutzungsversuche gab es vier Tage vor dem Patch, am Patchtag waren bereits mehrere Angreifer aktiv.

Geschäftsrisiko: Übernahme von Website, Shop oder Kundenportal mit Zugriff auf Datenbank, Zugangsdaten und API-Schlüssel – als Einstieg ins Netz, für Datenabfluss, Manipulation von Inhalten und einen ggf. meldepflichtigen Vorfall nach NIS-2 / DSGVO.

9,2 / 10

KRITISCH
CVSS 4.0 BASISWERT

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
– aus dem Netz, ohne Anmeldung und ohne Zutun – Code-Ausführung mit den Rechten des Webserver-Kontos. Hohe Angriffskomplexität, aber volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Gilt für beide CVEs (Bewertung des PHP-Security-Teams; kursierende 10,0 sind laut PHP Foundation falsch).

ANGRIFFSVERSUCHE SEIT
17.10.2026**BETROFFEN**
PHP 5.4 bis 8.5
jede Installation, die Webanfragen bedient**HANDLUNGSBEDARF**
Sofort – in Stunden

Das Wichtigste in 60 Sekunden.

9,2

KRITISCH · CVSS 4.0 · beide CVEs

Pre-Auth-RCE

vor jedem Anwendungscode

Seit 17.10.

Ausnutzungsversuche (Amazon)

PHP 5.4–8.5

jede Web-SAPI (FPM, mod_php, CGI ...)

Die Ursache: 109618: Gerät PHP beim Einlesen einer Anfrage in einen Speicherengpass, bleiben halb initialisierte Daten zurück, die beim Aufräumen als gültig gelten. **109619:** Zustand einer Anfrage überlebt die Freigabe seines Speichers (Use-after-free) und wird von der nächsten Anfrage am selben Worker genutzt. Folge: Code-Ausführung, bei 109619 auch Auslesen von Prozessspeicher.

ANGRIFFSKETTE

01

PHP erreichbar – beliebige Website oder Anwendung im Internet

02

Präparierte Anfrage – z. B. Multipart-Upload, der beim Einlesen einen Fehler auslöst

03

Speicher verdorben – PHP arbeitet mit ungültigem Zustand weiter

04

Code-Ausführung – Webshell, Datenzugriff, Auslesen von Geheimnissen

Betroffenheit & Fixversionen

PHP-Zweig	Verwundbar bis	Fixversion (Ziel)
8.5	< 8.5.12	8.5.12
8.4	< 8.4.27	8.4.27
8.3	< 8.3.36	8.3.36
8.2 (EoL 31.12.2026)	< 8.2.35	8.2.35
7.4 · 8.0 · 8.1	alle (EoL)	Backport-Quellcode / LTS-Anbieter
5.4 bis 7.3	alle (EoL)	kein Fix – Upgrade

Betroffen sind **alle Installationen, die Webanfragen bedienen**; höchstes Risiko laut PHP bei mod_php. Distributionen und LTS-Anbieter haben Pakete – Stand beim Anbieter bzw. Hoster prüfen, Appliances mit eingebautem PHP nicht vergessen.

Regulatorischer Hinweis: Ein bestätigter Zugriff auf eine Anwendung mit personenbezogenen Daten kann meldepflichtig sein – DSGVO i. d. R. 72 h, NIS-2 nach Ihren Fristen. Wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

Aug./Sep. 2026

Entdeckung, Meldung an PHP

CVE-2026-109618 · Überblick

17.10.2026

Erster Ausnutzungsversuch

20.10.2026

CVE-Nummern geleakt

21.10.2026

Patches veröffentlicht

Seite 3: Ihr Maßnahmenplan →

Ihr Maßnahmenplan.

In dieser Reihenfolge – Inventar vor Patch, Patch vor Entwarnung, Prüfung ab dem 17. Oktober.

SOFORT

Inventar + Patch (Stunden, nicht Tage)

WENN PATCH NICHT GEHT

Härten, isolieren, filtern

PARALLEL

Kompromittierung prüfen ab 17:10.

01

Alle PHP-Systeme finden

Websites, Shops, Portale, Intranet, aber auch Container-Images, Appliances und Control Panels mit eingebautem PHP. Je System Version und Betriebsart (FPM, mod_php, CGI) erfassen – bei gehosteten Seiten beim Hoster nachfragen.

02

Patchen und Worker neu starten

Auf 8.5.12 · 8.4.27 · 8.3.36 · 8.2.35 bzw. das Distributionspaket mit Fix. Danach **alle** PHP-Worker neu starten. 7.4 bis 8.1: auf eine unterstützte Version wechseln oder LTS-Backport einspielen.

03

Übergangsweise härten

Nur wenn der Patch nicht sofort geht – kein vollständiger Schutz: Upload-Fortschritt abschalten, `memory_limit` per `php_admin_value` festsetzen, Anfragegrößen und Multipart-Uploads am Webserver/WAF begrenzen, exponierte Altsysteme vom Netz nehmen.

04

Kompromittierung prüfen

Webserver- und PHP-Logs sichern und mindestens ab dem 17. Oktober auswerten – Sophos empfiehlt vorsorglich ab dem 1. August. Webroot auf neue Dateien (Webshells), Cronjobs, Konten und Prozesse prüfen, die PHP-Worker gestartet haben.

```
session.upload_progress.enabled = 0
```

05

Bei Verdacht: Geheimnisse wechseln

CVE-2026-109619 erlaubt das Auslesen von Prozessspeicher. Bei Hinweisen auf Ausnutzung Datenbank-Passwörter, API-Schlüssel, Tokens und Zertifikate der betroffenen Anwendung erneuern – ein Patch macht abgeflossene Zugangsdaten nicht wieder geheim.

Kompromittierungs-Indikatoren (IoCs)

ANFRAGEMUSTER

POST-Multipart mit
`PHP_SESSION_UPLOAD_PROGRESS`
danach Memory-Limit-Fehler / HTTP 500

HOST-AUFFÄLLIGKEITEN

`php-fpm` · `httpd` · `php-cgi` startet
`sh` · `bash` · `curl` · `wget` · `nc`
neue `.php`-Dateien im Webroot

QUELL-IPS (AMAZON, 17.–21.10.)

103.216.220.92 · 31.223.184.166
37.19.200.5 · 134.209.159.64
103.114.163.188 · 95.217.98.37

Zur Einordnung: Die IPs gehören zu Anonymisierungsdiensten, die auch legitime Nutzer verwenden – Amazon empfiehlt, Treffer zu untersuchen statt pauschal zu blockieren. Upload-Fortschritt und HTTP-500-Fehler kommen auch im Normalbetrieb vor; auffällig ist die Häufung. Fehlende Logeinträge sind kein Beweis für Sicherheit: Manche Fehler treten auf, bevor PHP etwas protokolliert.



Wichtig: Die Lücke liegt im PHP-Interpreter, nicht in WordPress, Drupal oder Ihrer Anwendung – ein CMS- oder Plugin-Update schließt sie nicht. Und ein Patch entfernt keine Webshell, die schon vorher abgelegt wurde. Weil es Versuche bereits vor der Veröffentlichung gab, gilt der 17. Oktober als spätester Startpunkt jeder Prüfung.

Vom Check bis zum Schutz – wir klären es schnell.

Patchen bleibt Pflicht. Ob vorher jemand drin war und wie Sie die nächste Lücke abfangen, klären wir mit Ihnen.



Forensik-Schnellcheck

Für selbst betriebene Server: Unser Forensik-Team prüft das laufende System auf Anzeichen einer Ausnutzung seit dem 17. Oktober – Logs, Webroot, Prozesse, Konten. Ergebnis: Befund je System.



Imageprüfung

Sie stellen uns ein Abbild (Image) Ihres Servers bereit; unser Forensik- und Malware-Team analysiert es in der Tiefe auf Webshells, Hintertüren und Schadcode. Mit schriftlichem Befund.



Web Application Firewall

Eine WAF auf Basis von OGO Security kann solche Angriffe abfangen, auch wo der Patch noch fehlt; laut OGO ist ein virtueller Patch gegen PHP2Shell aktiv. Bezug über Argos.

SO GEHEN WIR VOR

01 Forensik-Schnellcheck

Zeigt Ihr System Anzeichen eines Angriffs? Forensische Prüfung des laufenden Systems ab dem 17. Oktober.

02 Imageprüfung

Bei Verdacht oder für volle Gewissheit: Sie stellen das Server-Abbild bereit, unser Forensik- und Malware-Team analysiert es.

03 Absichern

WAF vor Ihre Anwendungen, laut Hersteller kurzfristig testbar.



Empfehlung für die Geschäftsleitung

- › Heute anordnen: alle PHP-Systeme inventarisieren und innerhalb von Stunden patchen – auch bei Hoster und Dienstleistern nachfragen.
- › Prüfen lassen, ob seit dem 17. Oktober ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- › Für Systeme, die sich nicht sofort patchen lassen (u. a. PHP 8.1 und älter), eine Web Application Firewall vorschalten und einen Ablösetermin festlegen.

Ihr Part · unser Part. Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.

Forensik-Schnellcheck und Imageprüfung umfassen die Feststellung auf dem jeweiligen System – Bereinigung und weitergehende forensische Maßnahmen gehören nicht dazu. Bei bestätigtem Vorfall übernimmt unser Incident-Response-Team · ISO/IEC 27001 (TÜV SÜD).

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Wir klären mit Ihnen, ob Sie betroffen sind und welches Paket passt.

+49 89 45 24 24-100 · sales@argos.security · www.argos.security



Termin buchen