Playbook php2shell

Sofortmassnahmen für PHP-basierte Systeme

Playbook php2shell
Swiss Infosec AG, Sursee

22.10.2026, Version 1.0

Swiss Infosec AG
Meienriesliweg 15
6210 Sursee

Tel +41 41 984 12 12
infosec@infosec.ch
www.infosec.ch

Beratung & Ausbildung
Informationssicherheit
Datenschutz
IT-Sicherheit
Krisenmanagement
BCM

Luzern
Bern
Zürich
Berlin

Playbook php2shell: Sofortmassnahmen für PHP-basierte Systeme

Management Summary

Am 21.10.2026 hat das PHP-Projekt zwei kritische Schwachstellen im PHP-Kern bekannt gemacht (CVE-2026-109618 und CVE-2026-109619, zusammengefasst als «php2shell»). Beide sind mit einem CVSS-Wert von 9.2 bewertet und erlauben die Ausführung von Schadcode aus der Ferne ohne vorherige Anmeldung. Betroffen ist PHP selbst, nicht einzelne Anwendungen. Damit sind alle Systeme gefährdet, die auf PHP laufen: Websites mit WordPress, TYPO3, Joomla oder Drupal, Online-Shops mit Magento oder Shopware, Nextcloud-Instanzen, Intranets, Formular- und Ticketsysteme sowie individuell entwickelte Webanwendungen.

Das Bundesamt für Cybersicherheit (BACS) und weitere nationale Behörden haben Warnungen herausgegeben. Zahlreiche Betreiber haben ihre Websites vorsorglich vom Netz genommen. Seit dem Nachmittag des 21.10.2026 stehen korrigierte PHP-Versionen zur Verfügung. Amazon stuft php2shell als breit ausgenutzt ein und sah den ersten Angriffsversuch bereits am 17.10.2026, vier Tage vor der Veröffentlichung. Hadrian meldet Ausnutzung in grossem Massstab, watchTowr aktive Angriffsversuche auf beide CVEs. Im CISA-KEV-Katalog stehen die Lücken noch nicht, bestätigte erfolgreiche Einbrüche sind bisher nicht publiziert.

Handlungsbedarf: sofort. Dieses Playbook führt in fünf Schritten durch Betroffenheitsanalyse, Sofortmassnahmen, Nachkontrolle, Meldepflichten und Kommunikation. Die Schritte 1 bis 3 sollten innert 24 Stunden abgeschlossen sein.

Schritt 1: Betroffenheit feststellen

Erstellen Sie eine Liste aller Systeme, die PHP ausführen. Denken Sie dabei auch an Systeme, die nicht als «Website» wahrgenommen werden.

Systemkategorie	Typische Beispiele	Zuständigkeit klären
Öffentliche Website	WordPress, TYPO3, Joomla, Drupal	Hoster oder Webagentur
Online-Shop	Magento, Shopware, WooCommerce, PrestaShop	Hoster, Shop-Betreiber
Kollaboration und Dateiablage	Nextcloud, ownCloud, Dateiaustausch-Portale	Interne IT oder Cloud-Anbieter
Intranet und Portale	Mitarbeiterportale, Kundenportale, Buchungstools	Interne IT, Softwarelieferant
Formulare und Fachanwendungen	Kontaktformulare, Bewerbungstools, Umfragen, Ticketsysteme	Fachbereich, Softwarelieferant
Infrastruktur-Werkzeuge	phpMyAdmin, Monitoring-Oberflächen, Wiki-Systeme	Interne IT

Für jedes System sind drei Fragen zu beantworten:

- Welche PHP-Version läuft (Hauptversion und Patchstand)?
- Wer ist für das Einspielen von Updates verantwortlich: eigene IT, Hoster, Agentur oder Lieferant?
- Ist das System aus dem Internet erreichbar oder nur intern?

Prüfen Sie zudem, ob Ihr Hoster bereits selbst reagiert hat. Mehrere Anbieter haben am 21.10.2026 vorsorglich Funktionen abgeschaltet oder Datei-Uploads über Websites gesperrt. Solche Massnahmen schützen nur teilweise; das Update bleibt erforderlich.

Schritt 2: Sofortmassnahmen innert 24 Stunden

Update einspielen

Die einzige vollständige Gegenmassnahme ist die Aktualisierung auf eine gepatchte PHP-Version. Patches stellt das PHP-Projekt für die unterstützten Versionsreihen 8.2, 8.3, 8.4 und 8.5 bereit. Nach dem Update ist der Webserver beziehungsweise der PHP-Dienst neu zu starten und die aktive Version zu verifizieren.

Nicht mehr unterstützte Versionen

Systeme mit PHP 8.1 oder älter (insbesondere 7.4, 7.3 und 5.6) werden vom PHP-Projekt nicht mehr unterstützt. Korrekturen gibt es nur als Quell-Backports (für 7.4 bis 8.1) oder als zurückportierte Pakete von Linux-Distributionen bzw. LTS-Anbietern. Liegt keine vom Anbieter bestätigte Korrektur vor, sind diese Systeme als kompromittierbar zu betrachten und sofort vom Netz zu nehmen oder zu isolieren. Anschliessend ist eine Migration auf eine unterstützte Version einzuplanen. Ein Weiterbetrieb mit Netzzugang ist nicht vertretbar.

Überbrückung bis zum Update

Kann das Update nicht umgehend erfolgen, gelten bis dahin folgende Überbrückungsmassnahmen:

- System vom Internet trennen oder hinter VPN beziehungsweise IP-Beschränkung stellen.
- Datei-Uploads und Formulare mit Anhängen temporär deaktivieren.
- Falls vorhanden: Web Application Firewall aktivieren und die vom Hersteller oder Hoster bereitgestellten Regeln für php2shell einspielen.
- Wartungsseite ohne PHP (statisches HTML) ausliefern, wenn der Betrieb für kurze Zeit unterbrochen werden kann.

Eine Website vorübergehend abzuschalten ist in der aktuellen Lage eine saubere und vertretbare Ent-scheidung. Ein kompromittierter Webserver dagegen zieht Datenverlust, Reputationsschaden, Haftungs-ansprüche und Meldepflichten nach sich. Halten Sie den Entscheid und die Begründung schriftlich fest.

Schritt 3: Nachkontrolle auf Kompromittierung

Nach dem Update ist zu prüfen, ob das System bereits vor dem Patch angegriffen wurde. Der relevante Zeitraum beginnt spätestens am 17.10.2026 (Vorankündigung durch das PHP-Projekt, erste Honeypot Angriffe am 17.10.2026 gemeldet) und reicht bis zum Abschluss des Updates.

- Webserver-Logs auf ungewöhnliche POST-Anfragen, Upload-Aufrufe und Zugriffe auf unbekannte PHP-Dateien prüfen.
- Dateisystem auf neu erstellte oder veränderte PHP-Dateien durchsuchen, insbesondere in Upload-, Cache- und Temp-Verzeichnissen (Hinweis auf Webshells).
- Benutzerverwaltung des CMS oder Shops auf neue Administratorkonten kontrollieren.
- Geplante Aufgaben (Cron) und Autostart-Einträge auf unbekannte Einträge prüfen.
- Ausgehende Netzwerkverbindungen des Servers auf unbekannte Ziele kontrollieren.
- Zugangsdaten rotieren: Datenbank-Passwörter, API-Schlüssel, SFTP- und Admin-Zugänge, sofern Anzeichen einer Kompromittierung bestehen.

Bei konkreten Hinweisen auf einen Angriff ist das System nicht zu bereinigen, sondern zu sichern (Abbild erstellen) und zu isolieren. Die gesicherten Daten dienen zugleich als Beweismittel für Meldungen an Behörden, für Ansprüche gegenüber Versicherungen oder Dienstleistern und für eine allfällige Strafanzeige. Die weitere Untersuchung erfolgt gemeinsam mit Ihrer IT und bei Bedarf mit der Swiss Infosec AG.

Schritt 4: Meldepflichten prüfen

Ergibt die Nachkontrolle eine Kompromittierung oder bestehen konkrete Anhaltspunkte dafür, sind insbesondere die folgenden Meldepflichten zu prüfen. Die Fristen laufen ab Entdeckung bzw. Kenntnisnahme, nicht erst ab Abschluss der Analyse:

Datenschutz Schweiz (Art. 24 DSG). Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Die Meldung nennt mindestens die Art der Verletzung, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen. Auftragsbearbeiter melden dem Verantwortlichen so rasch als möglich. Betroffene Personen sind zu informieren, wenn dies zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Bei einem kompromittierten Webserver mit Kundendaten, Bewerbungsunterlagen oder Gesundheitsangaben ist ein hohes Risiko regelmässig anzunehmen; im Zweifel

ist zu melden. Für öffentliche Organe von Kantonen und Gemeinden gilt das kantonale Datenschutzrecht, das teils eigene Meldepflichten vorsieht.

Datenschutz EU/EWR (Art. 33 und 34 DSGVO). Untersteht die Verarbeitung der DSGVO, etwa wegen einer Niederlassung im EWR oder weil sich Angebote an Personen im EWR richten, ist eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde zu melden. Die Schwelle liegt tiefer als nach Schweizer DSG: Die Meldung entfällt nur, wenn die Verletzung voraussichtlich zu keinem Risiko für die betroffenen Personen führt. Bei voraussichtlich hohem Risiko sind die betroffenen Personen zusätzlich unverzüglich zu benachrichtigen. Zuständig ist bei grenzüberschreitender Verarbeitung in der Regel die federführende Aufsichtsbehörde am Ort der Hauptniederlassung im EWR. Für Unternehmen ohne Niederlassung im EWR gilt dieses «One-Stop-Shop»-Verfahren nicht, auch wenn sie einen Vertreter nach Art. 27 DSGVO bestellt haben: Es ist sodann jede Aufsichtsbehörde der Mitgliedstaaten zu informieren, in denen betroffene Personen wohnen. Auftragsverarbeiter melden dem Verantwortlichen unverzüglich. Diese Meldungen erfolgen zusätzlich zu einer allfälligen Meldung an den EDÖB.

Cyberangriffe auf kritische Infrastrukturen (Art. 74a ff. ISG). Betreiber kritischer Infrastrukturen melden Cyberangriffe innert 24 Stunden nach Entdeckung dem BACS, wenn diese die Funktionsfähigkeit gefährden, zu einer Manipulation oder einem Abfluss von Informationen geführt haben, längere Zeit unentdeckt blieben oder mit Erpressung, Drohung oder Nötigung verbunden sind. Bereits eine eingeschleuste Webshell kann diese Kriterien erfüllen. Ob Ihre Organisation unter diese Pflicht fällt, ist vorab zu klären; dies betrifft unter anderem Behörden von Bund, Kantonen und Gemeinden, Hochschulen, Energie- und Wasserversorger, Entsorgungsbetriebe, Spitäler, Verkehrsbetriebe, Banken, Versicherungen, Kranken- und Unfallversicherer, Vorsorgeeinrichtungen, Cloud- und Rechenzentrumsanbieter sowie bestimmte Hersteller von Hard- und Software für kritische Infrastrukturen. Ob eine Organisation der Meldepflicht untersteht, beauskunftet das BACS auf Anfrage (Art. 74a Abs. 2 ISG). Die Erstmeldung erfolgt über den Informationen zum CSH oder über das Meldeformular auf dessen Website (siehe Informationen zur Meldepflicht).

Meldepflichten nach EU-Cybersicherheitsrecht (NIS-2, Cyber Resilience Act). Gesellschaften oder Niederlassungen in der EU, die unter die nationalen Umsetzungen der NIS-2-Richtlinie fallen, melden erhebliche Sicherheitsvorfälle innert 24 Stunden als Frühwarnung und innert 72 Stunden mit einer ersten Bewertung an das zuständige CSIRT bzw. die zuständige Behörde. Hersteller von Produkten mit digitalen Elementen, die auf dem EU-Markt bereitgestellt werden und PHP enthalten (z. B. Web-Oberflächen von Geräten), müssen seit dem 11.09.2026 aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle innert 24 Stunden nach Kenntnisnahme über die zentrale Meldeplattform der ENISA melden.

Weitere Melde- und Informationspflichten. Beaufsichtigte Finanzinstitute melden der FINMA Vorkommnisse von wesentlicher Bedeutung unverzüglich. Prüfen Sie zudem vertragliche Meldepflichten, insbesondere aus Auftragsbearbeitungsverträgen (ABV) mit Ihren Kunden, die oft kürzere Fristen vorsehen, sowie die Anzeigeobliegenheiten einer allfälligen Cyberversicherung: Viele Policen verlangen eine Meldung bereits im Verdachtsfall, teils auch die vorgängige Abstimmung mit dem Versicherer, bevor externe Dienstleister beigezogen werden.

Halten Sie ab sofort einen Zeitstrahl fest: Zeitpunkt der Kenntnisnahme, durchgeführte Massnahmen, Befunde. Diese Dokumentation ist Grundlage jeder Meldung und entlastet im Nachhinein. Halten Sie auch den Entscheid, keine Meldung zu erstatten, samt Begründung fest.

Schritt 5: Kommunikation

- Intern: Geschäftsleitung, IT und Datenschutzverantwortliche informieren; eine Person als Koordinationsstelle bestimmen.
- Lieferanten: Hoster, Agentur und Softwarelieferanten schriftlich um Bestätigung des Patchstands sowie um Mitteilung allfälliger Hinweise auf eine Kompromittierung bitten, mit Frist bis 22.10.2026.
- Kunden und Nutzende: nur bei Abschaltung oder bestätigtem Vorfall, kurz und sachlich, ohne technische Details, die weitere Angriffe erleichtern.
- Keine öffentliche Kommunikation über Angriffsdetails, bevor die Nachkontrolle abgeschlossen ist.

Checkliste

Nr.	Massnahme	Frist	Erledigt
1	Inventar aller PHP-Systeme erstellt, Zuständigkeiten geklärt	sofort	
2	PHP-Version je System ermittelt	sofort	
3	Gepatchte PHP-Version eingespielt und verifiziert	sofort	
4	Systeme mit PHP 8.1 oder älter vom Netz genommen oder isoliert	sofort	
5	Überbrückungsmassnahmen aktiv, wo Update noch aussteht	sofort	
6	Bestätigung des Patchstands von Hoster und Lieferanten eingeholt	innert 24 Std.	
7	Logs, Dateisystem und Benutzerkonten auf Kompromittierung geprüft	innert 48 Std.	
8	Zugangsdaten rotiert (bei Verdacht)	innert 48 Std.	
9	Meldepflichten (DSG, DSGVO, ISG, Aufsicht, Verträge, Versicherung) fristgerecht geprüft, Zeitstrahl dokumentiert	laufend	
10	Migrationsplan für nicht mehr unterstützte PHP-Versionen erstellt	31.10.2026	

Nachhaltige Massnahmen

php2shell zeigt exemplarisch, wie abhängig Webpräsenzen von einer einzelnen Komponente sind. Wir empfehlen, aus dem Vorfall vier dauerhafte Verbesserungen abzuleiten:

- Ein gepflegtes Inventar aller extern erreichbaren Systeme mit Softwareversionen und Verantwortlichkeiten.
- Einen Patch-Management-Prozess mit definierten Fristen für kritische Schwachstellen (Richtwert: 72 Stunden) und vertraglicher Verankerung bei Hoster und Agentur.
- Einen Lebenszyklus-Plan, der Betriebssysteme, Laufzeitumgebungen und CMS vor Supportende migriert.
- Einen Security Incident Prozess, der die Melde- und Informationspflichten mit Zuständigkeiten, Fristen und Vorlagen abbildet und regelmässig geübt wird.

Die Swiss Infosec AG unterstützt Sie unmittelbar bei der Betroffenheitsanalyse, der forensischen Nachkontrolle, der Beurteilung der Meldepflichten inkl. Kommunikation mit dem EDÖB, dem BACS oder ausländischen Aufsichtsbehörden, sowie bei der mittelfristigen Umsetzung der nachhaltigen Massnahmen.

Quellen

- PHP Security Team: Upcoming Critical PHP Security Release, Vorankündigung vom 20.10.2026
- Bundesamt für Cybersicherheit (BACS): Warnung zu kritischen Schwachstellen in PHP, 21.10.2026
- CVE-2026-109618 und CVE-2026-109619 (php2shell), CVSS 9.2
- Bundesgesetz über den Datenschutz (DSG, SR 235.1), Art. 24
- Informationssicherheitsgesetz (ISG, SR 128), Art. 74a ff.
- Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (FINMAG, SR 956.1), Art. 29 Abs. 2
- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), Art. 3, 27, 32–34 und 56
- Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), Art. 23
- Verordnung (EU) 2024/2847 (Cyber Resilience Act), Art. 14