VORFALL-LAGEBILD

PHP2Shell: Folgen für OT, Anlagen und Firewalls

Stand 05.11.2026 06:42, korrigiert 05.11.2026 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. PHP2Shell ist für die IT ein Patch-Thema, für die OT ein Inventar-Thema: Erst muss ich wissen, in welchen Geräten PHP steckt.

2. Das Webmenü einer Steuerung oder Firewall gehört nicht ins Internet und nicht ungefiltert ins Büronetz.

3. Kleine Teams schaffen das, wenn sie sich auf wenige Grundlagen konzentrieren: Inventar, Segmentierung, sicherer Fernzugang, Patchen nach Risiko.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
PHP hat am 21.10.2026 Fixes in den Versionen 8.2.35, 8.3.36, 8.4.27 und 8.5.12 veröffentlicht; ältere Stände dieser Zweige sind betroffen (bestätigt).	100 %	100 %	bestätigt
CVE-2026-109619 ist laut PHP-Advisory eine RCE über veralteten globalen Zustand zwischen zwei Anfragen an denselben Worker, CVSS v4.0 9,2, ohne Anmeldung (bestätigt).	100 %	90 %	präzisiert
CISA: Die Lücken erlauben Remote Code Execution ohne Anmeldung und betreffen alle PHP-Installationen, die Web-Anfragen bedienen (bestätigt).	100 %	95 %	bestätigt
Laut Datadog verarbeitet PHP die präparierte Anfrage, bevor Anwendungscode läuft; ein Login an der Anwendung schützt daher nicht (berichtet, Analyse eines Sicherheitsanbieters).	100 %	95 %	bestätigt
Laut Sansec stammt der fehlerhafte Code aus PHP 5.4.0 (2012); Calif fand die Pfade am 01.08.2026, Wiz meldete am 24.08.2026, Details sickerten am 20.10.2026 durch (berichtet).	100 %	85 %	offen
Die Veröffentlichung war für den 22.10. geplant und wurde nach dem Leak um einen Tag vorgezogen (berichtet).	100 %	70 %	offen
Die Lücke wurde mit Hilfe von KI-gestützten Audits gefunden und reproduziert.	75 %	100 %	bestätigt
BSI hat die Lage mit Warnstufe 3/Orange bewertet (berichtet; das PDF des BSI ließ sich technisch nicht auslesen).	100 %	100 %	bestätigt
CISA empfiehlt, PHP-Systeme, die nicht sofort aktualisiert werden können oder PHP 8.1 und älter nutzen, vom Netz zu nehmen, bis sie gepatcht sind (bestätigt).	100 %	95 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Palo Alto Networks: PAN-OS 10.2 bis 12.2 und Panorama sind betroffen, ein Fix ist noch nicht verfügbar (ETA offen); Übergangsschutz über Threat-Prevention-Signaturen und Beschränkung des Management-Interface (bestätigt).	100 %	5 %	widerlegt
OPNsense hat Hotfixes veröffentlicht: Community Edition 26.7.7 mit PHP 8.5.12, Business Edition 26.4.2p3 mit PHP 8.3.36 (bestätigt, offizieller Forumsbeitrag des Teams).	100 %	90 %	offen
Fortinet: FortiOS, FortiManager, FortiAnalyzer, FortiWeb, FortiSwitch, FortiNAC u. a. nicht betroffen; FortiADC, FortiSIEM, FortiSOAR, FortiClient EMS u. a. in Prüfung (bestätigt).	100 %	85 %	präzisiert
Sophos: keine Sophos-Produkte betroffen; das Lizenzportal MyUTM für die abgekündigte SG UTM lief auf betroffenem PHP und wurde offline genommen (bestätigt).	100 %	100 %	bestätigt
Laut Sansec kann die Lücke Geheimnisse aus dem Speicher preisgeben (Passwörter, Session-Tokens, API-Keys, TLS-Schlüssel) (berichtet).	100 %	80 %	offen
In DACH haben erste Stellen Webseiten vorsorglich abgeschaltet, u. a. Universität Genf, EPFL, Kanton Basel-Stadt; die Überschrift nennt Charité und Stadt Mainz (berichtet).	100 %	95 %	präzisiert
Viele OT-Geräte mit PHP-Webinterface laufen auf PHP-Versionen, für die es nur Quell-Patches gibt, und brauchen eine neue Firmware vom Hersteller.	65 %	75 %	präzisiert
Die unmittelbare Gefahr für OT besteht vor allem bei Geräten, deren Webinterface aus dem Internet oder aus dem Büronetz erreichbar ist.	80 %	85 %	präzisiert
Für normale Server stehen seit 21.10.2026 gepatchte PHP-Versionen bereit; Distributionen wie AlmaLinux liefern Pakete (bestätigt).	100 %	95 %	bestätigt
PHP 8.1 und älter bekommen keine offiziellen Binaries, nur Quell-Backports für 7.4, 8.0 und 8.1 (bestätigt durch Hersteller-Advisory von Sophos).	100 %	100 %	bestätigt
Workarounds (z. B. session.upload_progress.enabled=0, fatal_error_backtraces=0) senken das Risiko nur teilweise; nur der Patch behebt die Lücke (bestätigt).	100 %	100 %	bestätigt
Sophos empfiehlt, Aktivitäten ab dem 01.08.2026 zu prüfen, weil Dritte die Lücke möglicherweise früher kannten (bestätigt, Herstellerempfehlung).	100 %	100 %	bestätigt
Server mit aktuellem PHP sind innerhalb von Stunden bis wenigen Tagen gepatcht, Embedded-Geräte in Anlagen brauchen Wochen bis Monate.	70 %	80 %	präzisiert

Frühere Aussage	vorher	jetzt	Status
Wer kompromittiert wurde, muss mit Tagen bis Wochen für Forensik und Neuaufsetzen rechnen, weil Zugangsdaten aus dem Speicher abgeflossen sein können.	55 %	75 %	präzisiert

Neu seit dem letzten Stand

• PAN-OS: Hotfixes für alle Zweige zwischen 25.10. und 29.10.; aktive Ausnutzung gegen exponierte Managementoberflächen bestätigt.

• WAGO hat am 02.11. VDE-2026-132 veröffentlicht: CC100, Edge Controller, PFC100 G2, PFC200 G2, PFC300, TP600, WP400; Fix FW32 (4.10.4).

• Weitere OT-Advisories: B&R/ABB APROL, ABB MES und Netcontrol, Siemens RUGGEDCOM APE1808, Cisco URWB, Schneider Electric, Eaton, HMS, Welotec, Hitachi Energy, Johnson Controls; Moxa und Meinberg nicht betroffen; Rockwell in Prüfung.

• Unit 42 hat die Verbindung zu einem Vorfall bei einer europäischen Regierungsstelle am 25.10. zurückgezogen.

• KEV-Status widersprüchlich: SOCRadar/Abstract nennen Aufnahme am 26.10., nicht an CISA verifiziert.

• Neue, separate PHP-Schwachstelle CVE-2026-115560 (Session Upload Progress), nicht durch die Oktober-Releases behoben.

• Bei OTPulse wird ein Beitrag von OT-Cyber.de (dev.to) als Quelle für PHP in NetModule-, Mitsubishi-, Contec- und Kunbus-Geräten zitiert.

Wissensstand



■ Wissen 61 % ■ Wahrscheinlich 16 % ■ Nicht bekannt 23 %

PHP-Fixversionen, WAGO- und Palo-Alto-Advisory sowie die BSI-Warnstufe habe ich an der Primärquelle geprüft. Den KEV-Status und viele Herstellerlisten kenne ich nur aus Sekundärquellen, die sich zum Teil widersprechen.

1. Was ist passiert, und warum?

WISSEN

• PHP hat am 21.10.2026 die Versionen 8.5.12, 8.4.27, 8.3.36 und 8.2.35 mit den Fixes veröffentlicht; für PHP 8.1 und älter gibt es kein offizielles Release. (100 %)
[https://www.cms-admins.de/news/php2shell-kritische-php-sicherheitsluecken-cve-2026-109618/]

• Beide Lücken haben laut Berichterstattung je CVSS 4.0 Score 9,2 und erlauben Codeausführung ohne Anmeldung. (100 %)
[https://www.heidelberg24.de/verbraucher/php-sicherheitsluecke-bsi-warnt-vor-php2shell-was-jetzt-gilt-zr-94552990.html]

• watchTowr: auf Apache mod_php bestätigt, eine Anfrage ohne Anmeldung löst die Lücke aus, bevor Anwendungscode läuft. (100 %) [https://watchtowr.com/intelligence/php-cve-2026-109618-faq/]

• Der fehlerhafte Code reicht bis PHP 5.4 (2012) zurück. (100 %)
[https://www.engineering.com/php2shell-for-manufacturers-the-danger-goes-deeper-than-a-website/]

• CVE-2026-115560 (Session Upload Progress) ist eine eigene Lücke, die die Oktober-Releases nicht beheben. Sie greift nur, wenn session.serialize_handler auf php_binary oder php_serialize steht, die Anwendung ihn vor session_start() per ini_set() auf php umstellt und Upload Progress aktiv ist. Übergangsweise session.upload_progress.enabled=0 in php.ini bzw. im FPM-Pool setzen; das PHP-Team hält die Ausnutzung in der Praxis für unwahrscheinlich (100 %)
[https://www.it-connect.fr/php-cve-2026-115560-session-upload-progress/]

• Calif fand am 01.08.2026 im Rahmen der OpenAI-Initiative „Patch the Planet“ mehrere Wege zur Codeausführung und meldete am 11.08. an PHP; laut Calif halfen dabei ein LLM und Agenten, ohne Sondermodelle oder spezielle Werkzeuge (100 %) [https://calif.io/php2shell/]

• PHP Foundation: Das Calif-Audit lief ab 30.07.2026 im Programm „Patch the Planet“; Wiz meldete am 24.08. und OpenAI am 18.09. weitere Angriffswege, OpenAI fand dieselbe Ursache unabhängig (100 %)
[https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/]

• PHP Foundation: Erste Anzeichen des Speicherproblems (OOM) fielen 2024 bei der Arbeit an einem Befund des Quarkslab-Audits auf; ein möglicher Exploit wurde damals theoretisch erwogen, konkrete Angriffswege fand man aber nicht (100 %)
[https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/]

NICHT BEKANNT

• Wer die Details am 20.10. geleakt hat und wie.

• Ob Angreifer die Lücke schon vor dem Leak am 20.10.2026 ausgenutzt haben; das PHP-Team kannte das Grundproblem seit 2024, aber ohne konkreten Angriffsweg. SOCRadar meldet Ausnutzungsversuche ab dem 17.10.2026; die Seite konnten wir nicht selbst abrufen, die Angabe ist nicht unabhängig bestätigt.

• Die technische Ursache von CVE-2026-115560 und der Fix-Termin: PHP will das vollständige Advisory erst mit dem nächsten Release veröffentlichen.

2. Was ist die Auswirkung?

WISSEN

• BSI: Warnstufe 3 (Orange); wenn der Patch nicht sofort möglich ist, vorübergehende Trennung des Webservers vom Internet erwägen. (100 %)
[https://t3n.de/news/php2shell-sicherheitsluecke-php-bsi-warnung-1769356/]

• Palo Alto Networks: aktive Ausnutzung gegen aus dem Internet erreichbare PAN-OS-Managementoberflächen; Hotfixes für 10.2 bis 12.2 zwischen 25.10. und 29.10.2026. (100 %) [https://security.paloaltonetworks.com/CVE-2026-109618]

• Unit 42: rund 0,02 % der installierten Basis hatten betroffene, aus dem Internet erreichbare Managementoberflächen. (100 %) [https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/]

• WAGO VDE-2026-132 (02.11.2026): CC100, Edge Controller, PFC100 G2, PFC200 G2, PFC300, TP600 und WP400 mit Firmware unter 4.10.4 (FW32) betroffen; Fix FW32, für FW31 ein IPK-Sicherheitspatch; Übergangsweise Webserver abschalten. (100 %)
[https://certvde.com/en/advisories/VDE-2026-132]

• Siemens RUGGEDCOM APE1808 (läuft mit PAN-OS) betroffen, SSA-566512; 26 Siemens-Softwareprodukte laut SSA-566435 nicht betroffen (berichtet, Aggregator mit Link auf Siemens). (100 %) [https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

• B&R/ABB APROL bis R 4.4-65 betroffen (SA26P015), ABB MES mit DokuWiki-Hilfeserver betroffen, Cisco URWB betroffen (Fix 27.1.1 erst Februar 2027 erwartet), Moxa nicht betroffen (MPSA-260001), Rockwell in Prüfung (SD1802) (berichtet, Aggregator mit Links auf Herstellerseiten). (100 %) [https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

• Weitere Advisories bis 31.10.: ABB Netcontrol, Eaton, Hitachi Energy, HMS (Ixxat, Red Lion, Anybus Wireless u. a.), Welotec SMART EMS (VDE-2026-127), Wibu, Johnson Controls, Schneider Electric SESB-2026-295-01; Meinberg nicht betroffen (berichtet, Sammelliste). (100 %)
[https://patrickcoyle.substack.com/p/php-fallout-in-control-systems-10]

• Schneider Electric nennt laut SecurityWeek EcoStruxure Security Expert (Fix 1.48.4.0), ProLeiT LINEoptimize und EcoStruxure Control Engineering; eine andere Quelle nennt andere Produkte (widersprüchlich). (100 %)
[https://www.securityweek.com/industrial-vendors-check-products-for-php2shell-vulnerabilities/amp/]

• Charité, Unikliniken Freiburg, Heidelberg und Mannheim nahmen Webseiten vorsorglich vom Netz; Charité laut dpa am 21.10.: kein Cyberangriff, Betrieb nicht beeinträchtigt (berichtet). (100 %) [https://www.berliner-zeitung.de/article/10517112]

• Unit 42 schränkte seine Analyse in einem Update ein: Der Erstzugang bei einem beobachteten Angriff lasse sich den PHP2Shell-CVEs nicht sicher zuordnen (100 %)
[https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/]

NICHT BEKANNT

• Ob in DACH eine Anlage oder Steuerung über PHP2Shell kompromittiert wurde: dazu habe ich keine Meldung gefunden.

• Stellungnahmen von Phoenix Contact (TC ROUTER), Honeywell, Emerson, NetModule: nicht gefunden.

• Die PHP-Version in der WAGO-Firmware nennt das Advisory nicht.

WAHRSCHEINLICH (Einschätzung)

• Die unmittelbare Gefahr für OT besteht vor allem bei Geräten, deren Webinterface aus dem Internet oder dem Büronetz erreichbar ist. (85 %) – Die belegten Angriffe richten sich gegen exponierte Managementoberflächen (PAN-OS); WAGO empfiehlt, den Webserver abzuschalten.

• Weitere OT-Hersteller mit PHP-Webinterface werden in den nächsten Wochen Advisories nachschieben. (75 %) – Die Zahl der Advisories wächst wöchentlich; mehrere Hersteller mit dokumentiertem PHP haben sich noch nicht geäußert.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Workarounds wie session.upload_progress.enabled=0 schützen nicht vollständig; nur der Patch behebt die Lücke. (100 %) [https://securitylabs.datadoghq.com/articles/php2shell-critical-vulnerabilities-in-php/]

• Sophos: Keine Sophos-Produkte sind betroffen; nur das gehostete Lizenzportal MyUTM für die abgekündigte SG UTM lief auf betroffenem PHP und ist seit 21.10. offline. Für eigene exponierte Systeme empfiehlt Sophos vorsorglich, Aktivitäten ab dem 01.08.2026 zu prüfen (100 %)
[https://www.sophos.com/en-us/security-advisories/sophos-sa-20261021-php2shell]

• Palo Alto brauchte 4 bis 8 Tage nach dem PHP-Fix für Hotfixes aller Zweige. (100 %)
[https://security.paloaltonetworks.com/CVE-2026-109618]

• WAGO veröffentlichte sein Advisory am 02.11., 12 Tage nach dem PHP-Fix. (100 %)
[https://certvde.com/en/advisories/VDE-2026-132]

• CERT.at rät zu regelmäßigen Neustarts, damit Patches greifen (berichtet). (100 %)
[https://orf.at/stories/3445771/]

NICHT BEKANNT

• Wie viele Systeme vor dem Patch schon kompromittiert wurden.

• Wann Cisco URWB, Phoenix Contact und andere tatsächlich liefern.

WAHRSCHEINLICH (Einschätzung)

• Server mit aktuellem PHP sind innerhalb von Stunden bis wenigen Tagen gepatcht, Embedded-Geräte in Anlagen brauchen Wochen bis Monate. (80 %) – Belegte Spannen: PAN-OS 4 bis 8 Tage, WAGO 12 Tage, Cisco URWB Februar 2027; in Anlagen kommen Wartungsfenster dazu.

• Wer kompromittiert wurde, muss Zugangsdaten und Schlüssel tauschen, nicht nur patchen. (75 %) – Laut Sansec können Geheimnisse aus dem Speicher abfließen; ein Patch macht abgeflossene Daten nicht ungültig.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

• B&R betont, dass in APROL keine Ausnutzung gemeldet ist (berichtet). (100 %)
[https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

• Charité: Die Abschaltung der Webseite am 21.10. war vorsorglich wegen PHP2Shell, kein Angriff über PHP2Shell (berichtet) (100 %) [https://www.berliner-zeitung.de/article/10517112]

• Davon getrennt bestätigte die Charité am 30.10. einen Angriff auf ihren Webserver (Namen, E-Mail-Adressen, bei Beschäftigten Benutzernamen abgeflossen, keine Gesundheitsdaten); laut Charité steht er ausdrücklich nicht in Verbindung mit der PHP-Lücke (100 %)
[https://www.computerbase.de/news/wirtschaft/kritische-infrastruktur-hacker-stehlen-daten-der-berliner-charite.100094/]

NICHT BEKANNT

• Ob physische Schäden oder Produktionsausfälle durch PHP2Shell aufgetreten sind: kein Beleg gefunden.

WAHRSCHEINLICH (Einschätzung)

• Bisher geht es um Webseiten, Managementoberflächen und Gerätemenüs, nicht um zerstörte Anlagenteile. (80 %) – Alle belegten Fälle betreffen Web- und Managementzugänge; keine Meldung zu Prozessschäden.

• Ein Angreifer mit Zugriff auf eine Steuerung (z. B. PFC200 mit offenem Webinterface) könnte Konfiguration oder Programm verändern. (45 %) – WAGO nennt Kontrolle über den PHP-Prozess; wie weit das bis zur Steuerungslogik reicht, ist nicht belegt.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Cortex Xpanse zählte bei Veröffentlichung über 22,6 Millionen exponierte Instanzen (weltweit, PHP allgemein). (100 %) [https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/]

• Zscaler: 1.156 Angriffsversuche von 156 IPs gegen 70 Organisationen in den ersten 48 Stunden (eigenes Decoy-Netz). (100 %) [https://www.zscaler.com/blogs/security-research/cve-2026-109618-and-cve-2026-109619-php-vulnerable-unauthenticated-rce]

• Shodan (aggregiert, eigene Abfrage zum Stand 05.11.2026): OT-Protokolle öffentlich erreichbar in Deutschland: 143858 gesamt (DNP3 32879, OMRON FINS 26058, ProConOS 16086, EtherNet/IP 15935, Siemens S7 7782, OPC UA 5150). Diese Industrieprotokolle haben keinen direkten Bezug zu PHP; die Zahl zeigt nur, wie viel Anlagentechnik offen im Netz steht (100 %)

NICHT BEKANNT

• Wie viele OT-Geräte mit PHP-Webinterface in DACH aus dem Internet erreichbar sind: eigene Zählung nötig (Shodan), Ergebnis liegt mir nicht vor.

• Wie viele WAGO-, PAN-OS-, RUGGEDCOM- und APROL-Weboberflächen in Deutschland erreichbar sind: Unsere Shodan-Abfragen nach diesen Produkten lieferten keine verwertbare Zahl, weil die Produkte über Shodan nicht zuverlässig erkennbar sind.

WAHRSCHEINLICH (Einschätzung)

• In DACH sind mehrere tausend Industrie-Router und Steuerungen mit Webinterface aus dem Internet erreichbar, ein Teil davon mit PHP. (55 %) – Aus früheren Shodan-Auswertungen plausibel, für PHP2Shell aber nicht frisch gezählt.

6. Kann das wieder passieren?

WISSEN

• Mit CVE-2026-115560 ist bereits eine weitere, separate PHP-Schwachstelle bekannt, die die Oktober-Releases nicht beheben (berichtet). (100 %)

[https://www.it-connect.fr/php-cve-2026-115560-session-upload-progress/]

• Contec SolarView Compact wurde schon früher von Mirai-Botnetzen über das Webinterface ausgenutzt (Herstelleranalyse VulnCheck, nicht selbst geprüft). (100 %)

[https://www.vulncheck.com/blog/solarview-exploitation]

NICHT BEKANNT

• Ob weitere Kernfehler im selben Codebereich folgen.

WAHRSCHEINLICH (Einschätzung)

• Ungepatchte Embedded-Geräte bleiben über Jahre angreifbar, ähnlich wie nach Log4Shell. (80 %) – Lange Updatezyklen in OT, viele Geräte ohne Asset-Inventar; Muster aus Log4Shell.

Lage

Zwei kritische Schwachstellen im PHP-Kern (CVE-2026-109618, CVE-2026-109619) erlauben Remote Code Execution ohne Anmeldung. Seit 21.10.2026 gibt es Patches für PHP selbst, die Ausnutzung läuft, unter anderem gegen aus dem Internet erreichbare PAN-OS-Managementoberflächen. Mehrere OT-Hersteller haben inzwischen Advisories veröffentlicht (WAGO, B&R/ABB, Siemens, Cisco, Schneider Electric, HMS u. a.); viele Embedded-Geräte bekommen den Fix nur über eine neue Firmware.

Angriff	Massenhafte Ausnutzungsversuche gegen PHP-Webserver und PHP-basierte Managementoberflächen; bestätigte Ausnutzung gegen exponierte PAN-OS-Managementoberflächen.
Wann / Status	Leak 20.10.2026, Patches 21.10.2026, Angriffe ab spätestens 21.10.; ein Versuch am 17.10. laut Amazon (nur Sekundärquelle). · laufend
Täter	Nicht benannt; Unit 42 nennt keinen Threat Actor. – unbekannt
Betreiber / Branche	kein einzelner Betreiber; Hersteller und Betreiber weltweit · branchenübergreifend, OT: Automatisierung, Energie, Gebäudetechnik, Netzwerk/Firewall
Anlage / Alter	Steuerungen, HMI, Industrie-Router, Firewalls mit PHP-Webinterface · Code seit 2012; Geräte jeden Alters mit PHP
Region	weltweit, DACH
Auswirkungen	Bisher keine belegte Störung der Versorgung. Kliniken, Hochschulen, Stadtwerke und Verkehrsbetriebe (u. a. Saarbrücken) nahmen Webseiten vorsorglich vom Netz; Patientenversorgung laut Charité nicht betroffen.
Behörden	BSI (Warnstufe Orange), CERT.at mit dem neuen Bundesamt für Cybersicherheit (AT), CISA, CERT-EU, UK NCSC, NCSC-NL (Softwareliste), CSA Singapur.
Regulatorik	NIS2/KRITIS: Betreiber mit erheblichem Vorfall melden an BSI bzw. CERT.at/NCSC (Frühwarnung 24 h). CRA: Hersteller müssen ab 11.09.2026 aktiv ausgenutzte Schwachstellen in ihren Produkten an ENISA/CSIRT melden; das betrifft Geräte mit eingebettetem PHP (Einordnung, nicht juristisch geprüft).

Eingesetzte Produkte (öffentlich belegt)

• CC100, Edge Controller, PFC100 G2, PFC200 G2, PFC300, TP600, WP400 (WAGO) – Presse [https://certvde.com/en/advisories/VDE-2026-132]

• PAN-OS 10.2 bis 12.2, Panorama (Palo Alto Networks) – Presse [https://security.paloaltonetworks.com/CVE-2026-109618]

• RUGGEDCOM APE1808 (Siemens) – Presse [https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

• APROL bis R 4.4-65 (B&R / ABB) – Presse [https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

• Ultra-Reliable Wireless Backhaul (Cisco) – Presse [https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

• EcoStruxure Security Expert, ProLeiT LINEoptimize, EcoStruxure Control Engineering (widersprüchlich) (Schneider Electric) – Presse [https://www.securityweek.com/industrial-vendors-check-products-for-php2shell-vulnerabilities/amp/]

• SMART EMS (Welotec) – Presse [https://patrickcoyle.substack.com/p/php-fallout-in-control-systems-10]

• pfSense CE/Plus (Netgate) – Presse [https://www.otpulse.io/briefings/php2shell-ot-ics-impact-triage]

Angriffsvektor

Bekannt: Präparierte HTTP-Anfrage ohne Anmeldung an einen PHP-Prozess, der Web-Anfragen bedient (Details hier bewusst weggelassen).

• Aus dem Internet erreichbare Managementoberflächen von Firewalls und VPN-Gateways (hoch): Bestätigt bei PAN-OS; Edge Devices sind seit Jahren der bevorzugte Initial Access.

• Industrie-Router und Steuerungen mit offenem Webinterface (Fernwartung) (mittel): PHP im Webinterface belegt (WAGO, Phoenix Contact TC ROUTER laut Doku), Ausnutzung in OT aber nicht gemeldet.

• Monitoring-Server in der OT-DMZ (Zabbix, Cacti, Nagios XI) als Sprungbrett für Lateral Movement (mittel): PHP-Anwendungen, oft mit Zugangsdaten zu OT-Systemen, aber selten direkt im Internet.

Zeitleiste

2012 Fehlerhafter Code kommt mit PHP 5.4 in den Kern – berichtet
[https://www.engineering.com/php2shell-for-manufacturers-the-danger-goes-deeper-than-a-website/]

17.10.2026 Amazon meldet einen Ausnutzungsversuch vor der Veröffentlichung – berichtet
[https://socradar.io/blog/php2shell-cve-2026-109618-cve-2026-109619/]

20.10.2026, 22:21 PT Palo Alto liefert Threat-Prevention-Signatur (Threat ID 543004) – bestätigt
[https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/]

21.10.2026 PHP-Releases 8.5.12, 8.4.27, 8.3.36, 8.2.35; Universität Freiburg schaltet Webseiten, Intranet, ILIAS ab – bestätigt [https://www.berliner-zeitung.de/article/10517112]

22.10.2026 watchTowr: noch nicht im CISA-KEV-Katalog – bestätigt
[https://watchtowr.com/intelligence/php-cve-2026-109618-faq/]

25.10.2026 Unit 42 zieht Zuordnung eines Vorfalls bei einer europäischen Regierungsstelle zu PHP2Shell zurück – bestätigt [https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/]

25.10. bis 29.10.2026 PAN-OS-Hotfixes für alle Zweige – bestätigt
[https://security.paloaltonetworks.com/CVE-2026-109618]

26.10.2026 Aufnahme in CISA-KEV laut SOCRadar und Abstract Security (an CISA nicht verifiziert, widersprüchlich) – vermutet [https://socradar.io/blog/php2shell-cve-2026-109618-cve-2026-109619/]

29.10.2026 Unit 42 meldet aktive Ausnutzung gegen PAN-OS-Managementoberflächen – bestätigt [https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/]

02.11.2026 WAGO-Advisory VDE-2026-132 über CERT@VDE – bestätigt
[https://certvde.com/en/advisories/VDE-2026-132]

Vergleichsfälle

• Log4Shell (2021): Eine Bibliothek tief in fremder Software führt zu jahrelanger Nacharbeit, weil kaum jemand weiß, wo sie steckt. [https://en.wikipedia.org/wiki/Log4Shell]

• Contec SolarView, Mirai-Ausnutzung (2023 bis 2024): Offene Webinterfaces von Energiegeräten werden automatisiert und massenhaft angegriffen. [https://www.vulncheck.com/blog/solarview-exploitation]

Begriffe einfach erklärt

PHP: Eine Programmiersprache, mit der viele Webseiten und auch die Bedienmenüs vieler Geräte gebaut sind.

Remote Code Execution: Ein Angreifer kann aus der Ferne eigene Befehle auf dem Gerät ausführen.

Firmware: Die fest eingebaute Software eines Geräts, die nur der Hersteller aktualisieren kann.

OT: Die Technik, die Maschinen, Netze und Anlagen steuert, im Unterschied zur Büro-IT.

Edge Devices: Geräte am Übergang zum Internet, etwa Firewalls, VPN-Gateways oder Industrie-Router.

Früherer Stand: Erstmeldung (22.10.2026 07:30)

Wissen 55 % · wahrscheinlich 19 % · nicht bekannt 26 %
Am 21.10.2026 hat das PHP-Projekt zwei kritische Schwachstellen im PHP-Kern geschlossen (CVE-2026-109618, CVE-2026-109619, CVSS v4.0 je 9,2). Beide erlauben Remote Code Execution ohne Anmeldung, und Fixes gibt es nur für PHP 8.2 bis 8.5. Für OT ist entscheidend, dass PHP in vielen Webinterfaces von Steuerungen, Routern, Ladesäulen und Firewalls steckt; ob diese Geräte konkret ausnutzbar sind, haben die OT-Hersteller bisher nicht veröffentlicht.

Früherer Stand: Nach 72 Stunden (25.10.2026 06:38)

Wissen 56 % · wahrscheinlich 20 % · nicht bekannt 24 %

Zwei kritische Lücken im PHP-Kern (CVE-2026-109618, CVE-2026-109619, CVSS v4.0 je 9,2) erlauben Remote Code Execution ohne Anmeldung. PHP hat sie am 21.10.2026 behoben. Bis zum 25.10. gibt es viele Angriffsversuche, aber keine öffentlich bestätigte erfolgreiche Kompromittierung. Im OT-Umfeld haben bisher B&R/ABB (APROL, ABB MES), Siemens (RUGGEDCOM APE1808 mit PAN-OS), Palo Alto (PAN-OS), Cisco (URWB) und Peplink betroffene Produkte bestätigt. Moxa meldet keine betroffenen Produkte. Rockwell prüft noch. Von WAGO, Phoenix Contact, Schneider Electric, Honeywell und Emerson gab es bis zum letzten auffindbaren Stand keine Aussage.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.