

Update - School-CERT Sector Alert: Kwetsbaarheden in PHP

[TLP: **CLEAR**] Delen toegestaan

Prioriteit: Urgent
Categorie: Software webtechnologie
Leverancier: PHP

Context

Dit is een update op de eerdere Sector Alert van 21-10-2026, om je op de hoogte te houden van ontwikkelingen rondom de PHP-kwetsbaarheden.

Voor wie?

Deze melding is voor besturen die gebruik maken van PHP. Als jouw bestuur gebruikmaakt van PHP op servers die bereikbaar zijn vanaf het internet is deze melding relevant voor jou.

Naam	Kwetsbare versie(s)	Opmerkingen
PHP	Alle PHP-installaties die webverzoeken behandelen. Inclusief: - php-fpm - Apache met mod_php - php-cgi - FrankenPHP - LiteSpeed	CVE-2026-109618 (9.2 CVSS) CVE-2026-109619 (9.2 CVSS) Beide kwetsbaarheden kunnen leiden tot het uitvoeren van ongeautoriseerde code.

Wat is er aan de hand?

Er zijn twee kritieke kwetsbaarheden aangetroffen in alle PHP-softwareversies die gepubliceerd zijn vóór 21-10-2026 ([aankondiging vanuit PHP](#)). Deze twee kwetsbaarheden gelden voor alle PHP-installaties die niet de nieuwste update hebben. Omstreeks 15:50 uur heeft PHP nieuwe updates gepubliceerd. De updates zijn beschikbaar gesteld voor PHP versies 8.2, 8.3, 8.4 en 8.5. Controleer of jouw systemen kwetsbaar zijn aan de hand van onderstaande tabel:

Kwetsbaar	Update 21/10/2026	Opmerkingen
8.5.0 - 8.5.11	8.5.12	Kwetsbaarheden verholpen in nieuwste update volgens PHP
8.4.0 - 8.4.26	8.4.27	Kwetsbaarheden verholpen in nieuwste update volgens PHP
8.3.0 - 8.3.35	8.3.36	Kwetsbaarheden verholpen in nieuwste update volgens PHP
8.2.0 - 8.2.34	8.2.35	Kwetsbaarheden verholpen in nieuwste update volgens PHP
8.1.*	EOL	Sinds 31-12-2025 niet meer ondersteund; maar PHP heeft minimale broncodepatches beschikbaar gesteld
8.0.*	EOL	Sinds 26-11-2023 niet meer ondersteund; maar PHP heeft minimale broncodepatches beschikbaar gesteld
7.4.*	EOL	Sinds 28-11-2022 niet meer ondersteund; maar PHP heeft minimale broncodepatches beschikbaar gesteld
<7.3.*	EOL	Sinds 06-12-2021 niet meer ondersteund
5.*	EOL	Sinds 31-12-2018 niet meer ondersteund

De kwetsbaarheden kunnen aanvallers in staat stellen om op afstand ongeautoriseerde code uit te voeren, ook wel Remote Code Execution (RCE) genoemd. Afhankelijk van de manier waarop PHP wordt gebruikt, kan dit leiden tot de overname van de server.

Wat moet je doen?

We raden aan waar mogelijk systemen die PHP gebruiken van het internet los te koppelen, de update te installeren, en na verificatie van de update de systemen weer online te zetten. De beslissing om systemen van het internet los te koppelen moet voortkomen uit een interne risicoanalyse die gedaan wordt door bestuurders en ICT-verantwoordelijken.

Deze aanbeveling (om systemen tijdelijk van het internet los te koppelen) wordt gedaan om de volgende reden:

Door kwetsbare systemen tijdelijk offline te halen, kan de update veilig worden geïnstalleerd. Vervolgens kan worden gecontroleerd of de systemen nog goed functioneren en of de webserver daadwerkelijk gebruikmaakt van de bijgewerkte PHP-versie. Zo wordt voorkomen dat aanvallers de kwetsbaarheden tijdens het updateproces via het internet misbruiken.

Wanneer het niet mogelijk is systemen van het internet los te koppelen geldt de aanbeveling om de updates zo snel mogelijk door te voeren en te verifiëren dat de nieuwste versie draait.

Meer lezen

- <https://www.php.net/archive/2026.php#2026-10-20-1> (aankondiging updates)
- <https://www.php.net/> (vrijgeving updates ~15:50 21/10/2026)
- <https://www.php.net/downloads.php?source=Y>
- <https://cert.europa.eu/publications/security-advisories/2026-018/>
- <https://advisories.ncsc.nl/2026/ncsc-2026-0443.html>
- <https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
- <https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>

Wat kan je van ons verwachten?

We monitoren de situatie en brengen je op de hoogte als er ontwikkelingen zijn. Mocht de situatie aanleiding geven tot aanvullende acties dan informeren we je. Bij vragen of schade, neem gerust contact met ons op via cert@school-cert.nl.

Overzicht TLP-codes

School-CERT en partners maken gebruik van de TLP-standaard. Traffic Light Protocol (TLP) duidt op een simpele en intuïtieve manier wanneer en op welke wijze informatie mag worden verspreid. TLP maakt gebruik van kleurcoderingen: TLP:CLEAR, TLP:GREEN, TLP:AMBER en TLP:RED.

TLP:CLEAR (publiek) – geeft aan dat er geen beperkingen aan de verspreiding zitten. Je mag de informatie publiekelijk delen en op een openbaar toegankelijke website zetten.

TLP:GREEN (delen toegestaan) – de informatie mag uitsluitend onder gelijksoortige organisaties binnen de brede gemeenschap of sector gedeeld worden. Je mag het bijvoorbeeld wel publiceren op een gesloten internetforum, maar niet op een openbaar toegankelijke website.

TLP:AMBER (vertrouwelijk) – de informatie mag alleen gedeeld worden binnen de ontvangende organisatie (schoolbestuur) of met scholen die onder het bestuur vallen. Hierbij geldt het need to know-principe. De informatieverstrekker kan bij TLP:AMBER ook nog aanvullende beperkingen stellen.

TLP:RED (niet delen) – de ontvanger mag of de ontvangers mogen de informatie alleen delen met de informatieverstrekker en met de mede-ontvangers. De informatie is alleen voor de ogen van de ontvanger.

De verzender geeft de TLP-aanduiding duidelijk aan, bijvoorbeeld in het onderwerp van een e-mail, aan het begin van een tekst of in de hoofd- en voetnoot van een document.