



Advisory NCSC-2026-0443

PRIORITEIT: HOOG

Kwetsbaarheden verholpen in PHP

Publicatiedatum: 21-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

PHP heeft twee kritieke kwetsbaarheden verholpen. De kwetsbaarheden kunnen zonder authenticatie op afstand worden misbruikt voor het uitvoeren van willekeurige code. Alle PHP-installaties die webverzoeken verwerken zijn getroffen.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-109618 betreft geheugenbeschadiging bij de afhandeling van een Out-of-Memory-situatie. Hierdoor kunnen interne requestgegevens slechts gedeeltelijk worden geïnitieerd en tijdens de verwerking als geldige gegevens worden behandeld, wat kan leiden tot Remote Code Execution.

De kwetsbaarheid met kenmerk CVE-2026-109619 betreft het achterblijven van interne globale status nadat het bijbehorende geheugen is vrijgegeven. Een volgend verzoek dat door dezelfde worker wordt verwerkt, kan deze verouderde status gebruiken voordat deze opnieuw wordt geïnitieerd, wat eveneens kan leiden tot Remote Code Execution.

Beide kwetsbaarheden kunnen zonder authenticatie via webverzoeken worden misbruikt en kunnen leiden tot het uitvoeren van willekeurige code op de getroffen server. Het PHP-team adviseert alle gebruikers dringend om onmiddellijk te updaten. Het NCSC adviseert daarom de beveiligingsupdates met spoed toe te passen.

Oplossingen

Upgrade naar PHP 8.5.12, 8.4.27, 8.3.36 of 8.2.35. Gebruikers van Linux-distributies en LTS-versies wordt geadviseerd de door hun leverancier beschikbaar gestelde beveiligingsupdates toe te passen.

PHP 8.1 en ouder worden niet meer regulier door het PHP-project ondersteund. Voor PHP 7.4, 8.0 en 8.1 heeft het PHP-team vanwege de ernst van de kwetsbaarheden wel minimale broncodepatches beschikbaar gesteld.

Wanneer direct updaten niet mogelijk is, zijn tijdelijke mitigerende maatregelen beschikbaar voor beide kwetsbaarheden. Het PHP-team benadrukt dat deze maatregelen slechts specifieke aanvalspaden beperken en geen volledige oplossing vormen. Alleen het installeren van een beveiligingsupdate verhelpt de kwetsbaarheden volledig.

PHP heeft updates uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
- <https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>
- <https://www.php.net/>
- <https://www.php.net/downloads.php?source=Y>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-109618	
CVE-2026-109619	

CWE's

CWE	Beschrijving
CWE-416	Use After Free

Getroffen producten

Open Source
Open Source PHP

PHP

PHP

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:

NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.