Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0509

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in PHP

Publicatiedatum: 19-11-2026

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 de-len. 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

The PHP Group heeft meerdere kwetsbaarheden verholpen in PHP, specifiek in de PHP SOAP-extensie, session handling, HTTP stream wrapper, core netwerkfunctionaliteit, PHP-FPM, en PHP-CGI componenten.

Duiding

Een aantal kwetsbaarheden maakt het mogelijk voor ongeauthenticeerde remote aanvallers om heap geheugeninhoud te lekken via onjuist geïnitialiseerde arraypositions in de SOAP-extensie. Andere kwetsbaarheden in de session handling stellen aanvallers in staat om objectinjectie uit te voeren, wat kan leiden tot remote code execution of denial of service. Een use-after-free kwetsbaarheid in timezone cache kan leiden tot remote code execution. Er is een use-after-free conditie in PHP-FPM die lokale aanvallers met PHP-code uitvoering kan gebruiken om privileges te escaleren naar root. De HTTP stream wrapper kan door speciaal geconstrueerde HTTP headers leiden tot overmatig CPU gebruik en daarmee denial of service veroorzaken. Via een XSS kwetsbaarheid in PHP-FPM kan malafide JavaScript code worden geinjecteerd op in een browser van de beheerder. Verder veroorzaakt een fout in de verwerking van mixed-case HTTPS en FTPS URL's dat data onversleuteld wordt verzonden, wat kan leiden tot blootstelling van gevoelige informatie. De PHP-CGI binary bevat een kwetsbaarheid die out-of-bounds lees- en schrijfcondities mogelijk maakt, wat kan resulteren in crashes, geheugenlekken of geheugenbeschadiging. Tenslotte kan een use-after-free in de SOAP-extensie door crafted requests een crash van het PHP proces veroorzaken, wat denial of service tot gevolg heeft.

Oplossingen

PHP heeft updates uitgebracht voor versies 8.2.36, 8.3.37, 8.4.28 en 8.5.13 om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/php/php-src/security/advisories/GHSA-3mg3-cr28-46gc
- https://github.com/php/php-src/security/advisories/GHSA-4646-p932-gw34
- https://github.com/php/php-src/security/advisories/GHSA-5j3f-64r7-f564
- https://github.com/php/php-src/security/advisories/GHSA-658j-r8rw-q6mx
- https://github.com/php/php-src/security/advisories/GHSA-68fq-fh7h-f8gr
- https://github.com/php/php-src/security/advisories/GHSA-f6gg-rchx-xw8j
- https://github.com/php/php-src/security/advisories/GHSA-fm2m-fjf5-v3cp
- https://github.com/php/php-src/security/advisories/GHSA-g3vh-838c-65v7
- https://github.com/php/php-src/security/advisories/GHSA-gr4f-wgx5-jpfv

- https://github.com/php/php-src/security/advisories/GHSA-jm4m-qfqx-967m
- https://github.com/php/php-src/security/advisories/GHSA-mmf9-xm3v-hg2x
- https://github.com/php/php-src/security/advisories/GHSA-q23r-hr55-xmpg
- https://github.com/php/php-src/security/advisories/GHSA-qc49-hpvq-g2w6
- https://www.php.net/ChangeLog-8.php#8.2.36
- https://www.php.net/ChangeLog-8.php#8.3.37

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-15353	6.3 MEDIUM
CVE-2026-115560	9.2 CRITICAL
CVE-2026-126714	9.2 CRITICAL
CVE-2026-127960	8.7 HIGH
CVE-2026-128064	8.2 HIGH
CVE-2026-128090	7.7 HIGH
CVE-2026-129289	9.2 CRITICAL
CVE-2026-129291	8.8 HIGH
CVE-2026-129481	9.2 CRITICAL
CVE-2026-129506	6.3 MEDIUM
CVE-2026-129538	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-319	Cleartext Transmission of Sensitive Information
CWE-347	Improper Verification of Cryptographic Signature
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-407	Inefficient Algorithmic Complexity
CWE-416	Use After Free
CWE-444	Inconsistent Interpretation of HTTP Requests
CWE-459	Incomplete Cleanup
CWE-502	Deserialization of Untrusted Data
CWE-670	Always-Incorrect Control Flow Implementation
CWE-757	Selection of Less-Secure Algorithm During Negotiation
CWE-787	Out-of-bounds Write
CWE-823	Use of Out-of-range Pointer Offset
CWE-908	Use of Uninitialized Resource

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 of 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.