

# ‘Vertrouw me maar, bro.’ Een uiterst vaag bericht op een forum voor techneuten luidde de PHP-onrust in

Rik Wassens

De ellende begon dinsdagmiddag met een *post* op *Hacker News*, een forum voor techneuten. Daarin kondigde iemand een *patch* aan voor PHP, die liefst twee grote gaten zou dichten. De ‘pleister’ zou over twee dagen worden aangekondigd. „Ik heb geen bewijs”, [stond er in het bericht](#). „Vertrouw me maar, bro.”

Het bericht was uiterst vaag en de details klopten – achteraf gezien – niet helemaal. De datum van de aankondiging was onjuist, en de ernst van het lek was niet 10 (de hoogst mogelijke score), maar 9,2. Over de oorzaak van het lek waarop de pleister geplakt moest worden: geen woord. Alleen dat het tot *RCE* zou kunnen leiden: *Remote Code Execution*, het uitvoeren van commando’s op iemands anders systeem.

Het bericht op het forum en op sociale media was genoeg om hackers én beveiligers wereldwijd aan het werk te zetten. De een ging op zoek naar het lek in PHP, motor van 70 procent van alle websites, om dat zelf te kunnen uitbuiten. De ander probeerde het lek juist te dichten terwijl de patch nog ontbrak. In Nederland sneuvelen mediasites, DigiD.nl en zelfs de site van het NCSC, het Nationaal Cybersecuritycentrum. Die [ging korte tijd uit voorzorg op zwart](#).

Een select groepje cybersecurity-onderzoekers wist al maanden van de grote kwetsbaarheden in PHP. Alleen waren zij er niet in geslaagd het lek stil te houden tot de patch was verschenen. Met de grote onrust tot gevolg.

## Patch the planet

PHP is *open source* en wordt als programmeertaal wereldwijd veel gebruikt. Beheerder is een stichting met beperkte financiële middelen, die leunt op vrijwilligers. Dat leidt tot groeiend ongemak, nu steeds geavanceerdere AI het steeds eenvoudiger maakt bugs op te sporen in inmiddels decennia oude computercode.

Deze zomer werd PHP dan ook opgenomen in ‘[Patch the Planet](#)’, een initiatief van AI-gigant OpenAI, dat „de kritieke opensourcesoftware moet versterken waar de wereld van afhankelijk is”. Sinds eind juli speurden beveiligingsonderzoekers van onder andere het Amerikaanse Calif al naar gaten in PHP.

Op 11 augustus vonden zij met behulp van de nieuwste *AI-frontier*-modellen, de eerste van uiteindelijk twee lekken in PHP. Toen volgde – in vaktermen – een *coordinated vulnerability disclosure*. Het lek moet dan stap voor stap geverifieerd worden, een pleister moet worden bedacht, gemaakt en getest, en daarna moet een plan worden opgesteld om die snel te verspreiden onder álle gebruikers en versies van de systemen.

Het is een race tegen de klok. Zolang de patch niet verspreid is, zijn immers alle systemen kwetsbaar. Geheimhouding is cruciaal; als ook maar iets uitlekt, kunnen hackers gericht zoeken naar de gaten. En als ze

die vinden en succesvol weten uit te buiten vóór de patch beschikbaar is, volgt een doemscenario: alle systemen zijn kwetsbaar, en een sluitende oplossing ontbreekt. En AI maakt lekken vinden steeds makkelijker.

Deze week ging dat mis en dreigde het lek zélf uit te lekken. „De gecoördineerde *disclosure* verliep goed, tot twee dagen voor de geplande publicatiedatum van de patch”, schreef [de PHP-stichting woensdagmiddag](#). Nadat de naderende patch was uitgelekt, besloot de stichting de aankondiging ervan én de patch zelf te vervroegen. „Dat was het beste compromis tussen snel handelen, mensen tijd geven om voorbereidingen te treffen, en ervoor zorgen dat iedereen vervolgens snel kon updaten.”

Vervolgens publiceerde Calif dinsdagavond per ongeluk een video die het lek demonstreerde. Die toonde, onder [een stevige beat en met dansende cartoonpoppetjes](#), hoe de beveiliging van het ene na het andere PHP-platform – WordPress, MediaWiki, phpBB, Magento – binnen luttele seconden bezweek. De video liet zo de kwetsbaarheid zien van talloze websites en webwinkels die deze platformen gebruiken.

Hoewel de video vaag was, bevatte hij wél aanknopingspunten voor hackers. Uren voor publicatie van de patch schond een beveiligingsbedrijf ook nog eens het embargo door deze al te verspreiden – ook naar alle aanvallers, die meekeken. „Hiermee werd weken werk door vele partijen ongedaan gemaakt”, meldde de stichting achter PHP.

Door alle lekken zag Cloudflare, dat grote delen van het internet beveiligt, al duizenden pogingen om de kwetsbaarheid te misbruiken in de uren vóór de patch publiek zou worden. „Dat sprong naar tienduizenden in de 45 minuten na de [officiële] aankondiging [van de patch], naar honderdduizenden binnen twee uur, naar miljoenen nu”, zei Cloudflare-ceo [Matthew Prince donderdag op X](#).

Mogelijk lekten details van de hack nog eerder uit. AWS Security, de beveiligingstak van de Amerikaanse cloudgigant Amazon, [detecteerde al op 17 oktober](#) een poging om het lek in PHP te misbruiken. Dat was vier dagen voor de aankondiging.

## ‘Eén werkende variant is genoeg’

De vraag is hoe makkelijk het lek in PHP écht uit te buiten is. Hoewel online allerlei scripts rondgaan waarmee ingebroken kan worden, en er veel ‘aanvalsverkeer’ gezien wordt, heeft het Nederlandse Cybersecuritycentrum na onderzoek nog geen succesvol misbruik gezien, meldde [het donderdagmiddag](#). „Dat sluit toekomstig misbruik niet uit. Eén werkende variant kan voldoende zijn om aanvallen op grotere schaal mogelijk te maken.”

Zonder AI was het lek niet eenvoudig uit te buiten geweest, schreef cybersecuritybedrijf Wiz (een andere betrokken partij) [in een onderzoeksrapport](#). Want simpel is dat inderdaad niet. „Om de fouten te misbruiken is een zeer complexe serie handelingen nodig, op de grens van wat menselijke onderzoekers in de praktijk kunnen uitvoeren.”

De specifieke kwetsbaarheid in PHP werd in 2020 en 2024 al gedetecteerd, maar tot een oplossing kwam het nooit. Door beperkte capaciteit en onenigheid bleef een oplossing te lang liggen, erkende de PHP-stichting

woensdag. „We ontkennen niets. De vertraging was een structurele tekortkoming, veroorzaakt door ons besluitvormingsproces en een gebrek aan middelen.”

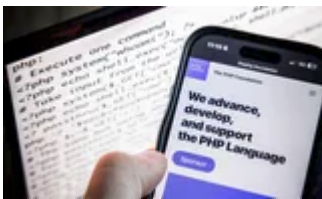
De zwakke plekken in PHP hebben hun oorsprong in de manier waarop de programmeertaal computergeheugen aanwendt, schrijft Wiz. Zulke aanvallen zijn notoir lastig te generaliseren, want iedere PHP-installatie is net anders. Maar AI maakt daar nu korte metten mee, aldus Wiz. Kwetsbaarheden die ooit onmogelijk of te tijdrovend waren voor misbruik, kunnen dankzij AI toch benut worden, waarschuwt het bedrijf. „Tegelijkertijd geven deze mogelijkheden ook verdedigers de kans om fouten te ontdekken die jarenlang niet opgemerkt zijn.”

Achteraf is het altijd makkelijk praten, zegt cybersecurity-expert Matthijs Koot. „Het rommelige traject heeft wel bijgedragen aan de paniek en de chaos. Maar ook zonder alle ruis is het vaak even rennen en gillen voordat alles gepatcht is. Als het lek inderdaad lastig uit te buiten is, dan is dat een meevaller, want alles wees op het tegendeel: het aanvalsverkeer dat Cloudflare al vroeg zag en de hoge scores die de kwetsbaarheid kreeg toegekend.”

We zijn door het oog van de naald gekropen, zegt Koot. „Het verschijnen van *exploit code* voordat de patch er is, is een horrorscenario. ”

[Lees ook](#)

[De problemen rond programmeertaal PHP worden het ernstigste cyberlek in jaren genoemd. Wat is er aan de hand?](#)



## Maak NRC jouw voorkeursbron op Google

Bij Google kan je nu zelf aangeven welke nieuwsbronnen jij vaker wil zien in je zoekresultaten. [Meer informatie](#)

[Kies NRC als voorkeursbron](#) Melding voorkeursbron sluiten