



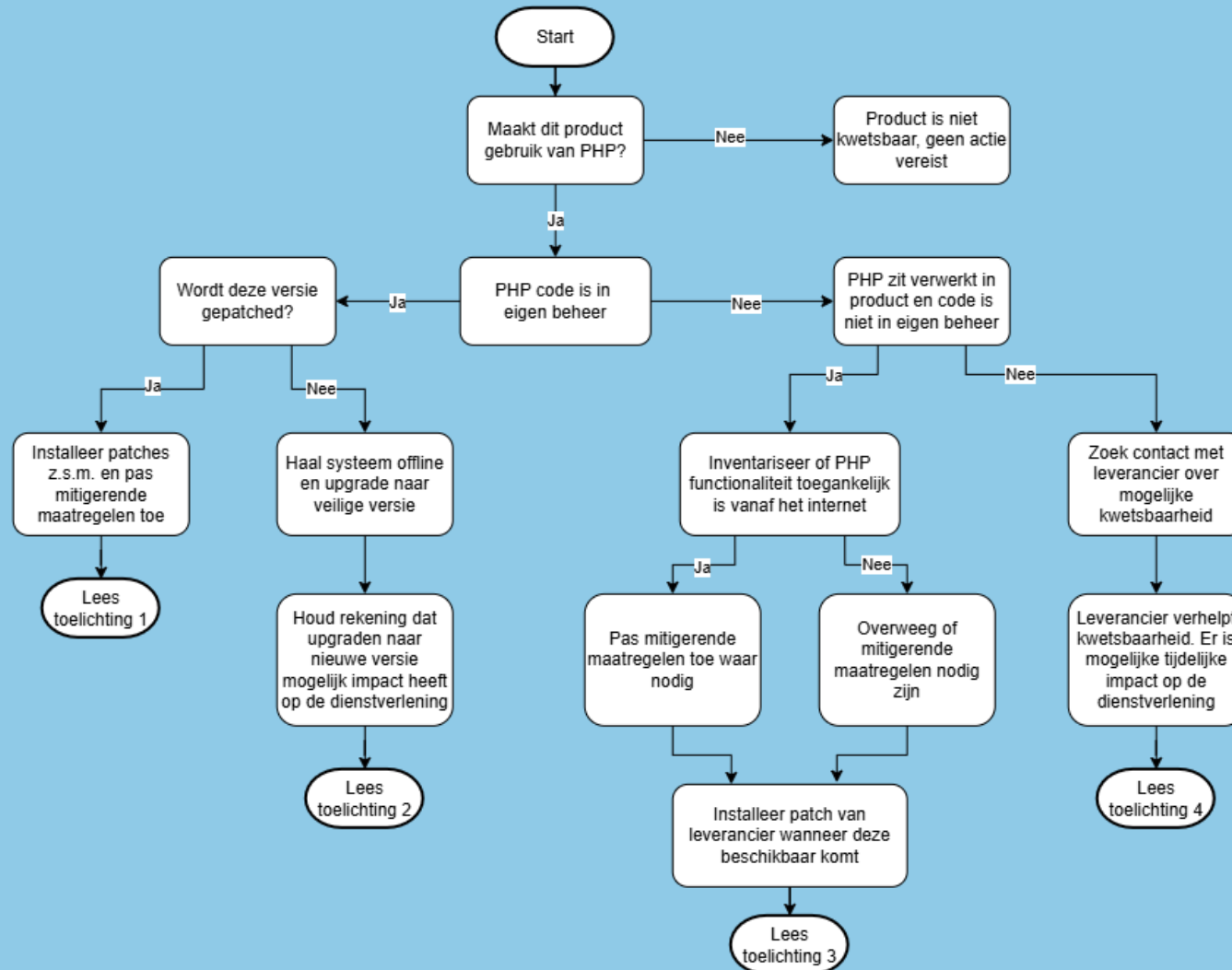
Handreiking

Beslisboom + toelichting: 'PHP-kwetsbaarheden: wat kan je doen?'

21-10-2026



Beslisboom



Toelichting bij de beslisboom

1 - PHP is in eigen beheer, versie 8.	Momenteel maak jij als organisatie gebruik van PHP-versie 8.2 en hoger, het product in eigen beheer. Wees dan aandachtig voor de volgende punten: Voor PHP versie 8 verschenen op woensdag 21-10-2026 patches. Installeer deze patches zo snel mogelijk. Duiding ▪ Wordt er een recente versie van PHP v8.2 en hoger gedraaid dan kan er z.s.m. worden gepatcht waarna eventueel onderzoek opgestart moet worden naar mogelijk misbruik. ▪ Houd rekening met vertraging van de dienstverlening van jouw organisatie door de mitigerende maatregelen voor de patch, en het onderzoek naar misbruik na de patch. ▪ Als mitigerende maatregelen zijn meerdere opties mogelijk met als meest impactvolle maatregelen het tijdelijk offline halen van systemen totdat patches zijn geïnstalleerd.
2 - PHP is in eigen beheer, versie is verouderd.	Momenteel maak jij als organisatie gebruik van een verouderde versie van PHP <v8.2 en je hebt het product in eigen beheer. Wees dan aandachtig voor de volgende punten: • Als het een PHP-product is dat je in eigen beheer hebt, maar niet gepatcht gaat worden aangezien het een versie betreft die niet in de patch zit, haal dan het betreffende product offline. • Dit is essentieel omdat zolang het product vanaf het internet benaderbaar is, er actief misbruik gemaakt kan worden van de geldende kwetsbaarheden. • Het wordt aangeraden om zo snel mogelijk te upgraden naar de nieuwste gepatchte PHP-versie en daarna het onderzoek naar mogelijk misbruik op te starten. • Online blijven/gaan zonder upgrade is zeer risicovol omdat de kwetsbare PHP-versies momenteel pogingen tot misbruik ervaren. • Upgrade daarom pas voordat je online gaat, dit kan verschillende neveneffecten hebben gezien de onderlinge communicatie kunnen systemen anders op elkaar gaan reageren op nieuwe PHP-versies. Duiding: • Organisaties die gebruik maken van oude PHP-versies die niet gepatched gaan worden zullen de meeste downtime ervaren. Voor PHP-versies <v8.2 wordt geen patch uitgebracht. Daarom is het van belang dat deze systemen zo snel mogelijk offline worden gehaald. Om te voorkomen dat de kwetsbaarheid in

	deze oude PHP-versie wordt misbruikt dient er te worden geüpgradet naar een veilige versie die niet kwetsbaar is. • Een upgrade naar een nieuwe PHP-versie kan zorgen voor conflicten met andere software die je binnen jouw organisatie draait. Houdt hier rekening mee. Dit kan namelijk voor langere impact op de beschikbaarheid van jouw systeem of applicatie zorgen.
3 - Product dat PHP gebruikt is in eigen beheer, PHP-code zelf niet.	Momenteel maak jij als organisatie gebruik van een product dat PHP gebruikt, je hebt de PHP-code zelf niet in eigen beheer, maar het product waar PHP in gebruikt wordt wel. Wees dan aandachtig voor de volgende punten: • Kijk of de PHP-functionaliteit van buitenaf toegankelijk is. Bijvoorbeeld als een webinterface een edge device PHP gebruikt om inloggen mogelijk te maken. • Als dit het geval is neem dan passende mitigerende maatregelen op basis van een risicoinschatting. Als dit niet het geval is overweeg dan alleen of mitigerende maatregelen nodig zijn. • Vervolgens is het belangrijk om te wachten tot dat de leverancier met een patch uitkomt. Installeer deze zo snel mogelijk. Duiding: • PHP kan in veel verschillende type producten toegepast worden. Het is belangrijk dat organisaties zelf weten wat voor type product PHP gebruikt en wat de functionaliteiten zijn. Op basis daarvan kan de desbetreffende organisatie een risicoafweging maken om te kijken indien de PHP-functionaliteit van buiten af benaderbaar is wat de meest passende maatregelen zijn. Als de functionaliteit niet van buitenaf te benaderen is dan is maak dan alsnog een risico overweging omtrent mogelijke mitigaties.
4 - Zowel het product dat gebruik maakt van PHP, als PHP zelf zijn niet in eigen beheer.	Momenteel maak jij als organisatie gebruik van een product dat PHP gebruikt maar de PHP-code zelf en het product waar PHP op draait zijn beide niet in eigen beheer maar worden afgenomen van een externe partij (bijvoorbeeld een cloudproduct). Wees dan aandachtig voor de volgende punten: • Het is belangrijk om in contact te komen met de leverancier om de aard van de kwetsbaarheid te achterhalen. • De leverancier zal met een nieuwe versie van het product komen waarin de kwetsbaarheden verholpen zijn. Duiding: • Houd rekening met mogelijke impact op de dienstverlening totdat de leverancier de kwetsbaarheden verholpen heeft. Stel hier eventueel vragen over aan je leverancier en bereid je hierop voor.

Waar gaan we naar toe?

Het NCSC verwacht dat de huidige PHP-situatie langdurig aandacht behoeft. Doordat gebruik van PHP zo breed verspreid is en in een grote categorie aan verschillende producten zit, zal het enige tijd duren voordat het grootste deel van de kwetsbare systemen en producten geüpdatet is naar een veilige versie.

Daarnaast zal ook het upgraden van oudere versies (PHP 5.x en 7.x) die End-of-Life (EOL) zijn tijd kosten en impact hebben op gekoppelde applicaties en functionaliteiten. Dit betekent dat er een langdurige periode volgt waarin kwaadwillenden kwetsbare systemen en organisaties kunnen identificeren en digitale aanvallen kunnen uitvoeren.

Ook zullen systemen van leveranciers die gebruik maken van PHP niet meteen een patch beschikbaar hebben maar moeten ze de door PHP beschikbare patches eerst intern toetsen op hun product. Hierdoor kunnen patches van producten die gebruikmaken van PHP een vertraging hebben. Organisaties moeten daarom overwegen of mitigerende maatregelen nodig zijn.

Ervaringen uit het verleden met een vergelijkbare kwetsbaarheid in log4j (log4shell) laten zien dat aanvallers een lange periode de kwetsbaarheid blijven misbruiken. Het is waarschijnlijk dat dit voor deze kwetsbaarheden in PHP ook het geval zal zijn.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)

Oktober 2026