26643 Informatie- en communicatietechnologie (ICT)

Nr. 1574 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 oktober 2026

Als coördinerend bewindspersoon op cybersecurity informeer ik uw Kamer, mede namens de staatssecretaris Digitale Economie en Soevereiniteit en de staatssecretaris Binnenlandse Zaken en Koninkrijksrelaties, over twee kwetsbaarheden in Hypertext Preprocessor (PHP).

Kwetsbaarheden PHP
Het Nationaal Cyber Security Centrum (NCSC) is via een internationale partner over de kwetsbaarheden in PHP geïnformeerd. Deze kwetsbaarheden zijn een weeffout in de software. Met de kwetsbaarheden in PHP zouden kwaadwillenden op afstand commando's kunnen uitvoeren, ook wel Remote Code Execution (RCE) genoemd, op iedere site/webserver en systemen waarop PHP draait. Het gevolg daarvan kan zijn dat de (web)servers overgenomen kunnen worden en websites niet meer toegankelijk zijn, of gegevens worden gelekt.

De kwetsbaarheden treffen daarnaast niet alleen websites, maar ook een grote diversiteit aan andere producten. Hier zitten oudere versies van PHP bij die niet meer worden voorzien van nieuwe updates of patches omdat ze reeds end-of-life zijn. Alle versies van PHP, in ieder geval versie 5 en hoger, zijn kwetsbaar. Daarmee zijn alle producten en componenten waar PHP in zit of wat gebruik maakt van PHP in potentie kwetsbaar. Dit betekent dat het van belang is dat organisaties zicht hebben op afhankelijkheden van PHP in de toeleverancierskeketen.

Op basis van het signaal van de internationale partner, hebben experts van het NCSC onderzoek gedaan en advies en handelingsperspectief ontwikkeld voor gebruikers van PHP. Toen de kwetsbaarheden vroegtijdig bekend werden, kon NCSC doelgroepen hierdoor snel informeren over deze adviezen. Dit heeft ertoe geleid dat veel organisaties preventief hun website en systemen offline hebben gehaald, ook in andere landen wordt aan organisaties het advies gegeven om systemen preventief offline te halen. Het is goed om te zien dat veel organisaties de adviezen van het NCSC opvolgen, ook al zijn deze maatregelen niet zonder impact.

De precieze maatschappelijke impact van deze kwetsbaarheden is op dit moment niet duidelijk. De impact wordt op dit moment onderzocht en nauwgezet gevolgd. Op dit moment worden de eerste internationale signalen van mogelijk misbruik ook onderzocht door het NCSC. Verdere signalen over misbruik zijn aannemelijk, aangezien er al zogenoemde Proof of Concepts (PoC’s) bekend zijn. Dat betekent dat aangetoond is dat de kwetsbaarheid misbruikt kan worden. Door gebruik van artificiële intelligentie (AI) kunnen

deze kwetsbaarheden mogelijk nog sneller worden misbruikt. Het NCSC blijft dit actief monitoren en staat hierbij in nauw contact met internationale partners.

Gistermiddag 21 oktober is er een patch beschikbaar gekomen voor de laatste versie van PHP. Het NCSC adviseert organisaties om zo snel mogelijk te patchen. Het advies geldt ook voor Rijksoverheidsorganisaties. Softwareleveranciers en organisaties moeten nu deze updates verwerken in hun systemen. Patchen kan tijd vergen, waardoor het risico niet bij iedereen direct gemitigeerd zal zijn. Ook de digitale dienstverlening van Rijksoverheidsorganisaties kan hierdoor beïnvloed worden totdat de patch is verwerkt. Tegelijkertijd hebben veel Rijksoverheidsorganisaties de update verwerkt, waardoor veel organisaties die preventief hun website en systemen offline hebben gehaald weer bereikbaar zijn. Verder heeft het NCSC een webinar georganiseerd om de doelgroep te informeren en een beslisboom gepubliceerd die door organisaties gebruikt kan worden om te beoordelen welke handelingen nodig zijn.

Versterken weerbaarheid
Zoals dit incident laat zien, kent de digitale wereld bekende en onbekende kwetsbaarheden. Het blijft daarom van belang om de basismaatregelen die het NCSC adviseert op orde te hebben, zodat tijdig en adequaat gereageerd kan worden op kwetsbaarheden en incidenten, voor zowel bedrijven, de Rijksoverheid als voor decentrale overheden. Daarnaast blijft het kabinet inzetten op het permanent versterken van onze cyberweerbaarheid. Bijvoorbeeld via de recentelijk ingevoerde Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten, en via de Wet bevordering digitale weerbaarheid bedrijven. Sinds de inwerkintreding van laatstgenoemde wet informeert het NCSC ook niet-vitale bedrijven over digitale kwetsbaarheden. De Cyber Resilience Act verplicht fabrikanten actief misbruikte kwetsbaarheden in producten met digitale elementen te melden en, vanaf 11 december 2027, om deze producten secure-by-design op de markt te brengen en kwetsbaarheden onverwijld te verhelpen.

De implementatie van de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) is en blijft een belangrijke basis voor het versterken van onze digitale weerbaarheid. De veranderende dreiging en de opkomst van nieuwe technologieën, waaronder AI, vraagt echter om een aanpassing aan een nieuwe realiteit. Daarom komt het kabinet met een actieprogramma “Toekomstbestendige Digitale Weerbaarheid” waarover ik uw Kamer op korte termijn zal informeren.

Tot slot
Deze situatie onderstreept het belang om als Nederland digitaal weerbaar te blijven. Weerbaarheid begint door de basis op orde te hebben: breng risico’s in kaart, bevorder veilig gedrag, bescherm systemen, applicaties en apparaten, beheer toegang tot data en diensten, en wees voorbereid op incidenten.

De minister van Justitie en Veiligheid,

D.M. van Weel