Ministerie van Justitie en Veiligheid

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Cybersecurity en Statelijke dreigingen
Cybersecurity

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.rijksoverheid.nl/jenv

nota

Kamerbrief kwetsbaarheden PHP

Datum
22 oktober 2026

Bijlage(n)
1

Bijlage(n)

1. Kamerbrief kwetsbaarheden PHP

1. Aanleiding

Er zijn twee kwetsbaarheden bekend gemaakt in PHP waarna het NCSC organisaties heeft geadviseerd uit voorzorg hun website offline te halen en zo snel mogelijk te patchen. Deze kwestie onderstreept het belang van het versterken van onze digitale weerbaarheid.

2. Geadviseerd besluit

U wordt geadviseerd om, vanuit uw coördinerende rol op cybersecurity, bijgevoegde Kamerbrief over de kwetsbaarheden in PHP, mede namens de staatssecretaris van Economische Zaken en Klimaat (vanwege de verantwoordelijkheid voor het bedrijfsleven) en de staatssecretaris van Slagvaardige Overheid en Koninkrijksrelaties (vanwege de verantwoordelijkheid voor de Rijksoverheid), te verzenden naar de Tweede Kamer.

3. Kernpunten

- Het NCSC is door een internationale partner geïnformeerd over twee kwetsbaarheden in PHP en was daardoor in staat om organisaties tijdig te informeren. Dit heeft ertoe geleid dat veel organisaties preventief hun website en systemen offline hebben gehaald. Deze kwetsbaarheid is geen aanval, maar een weeffout in de software.
- Deze maatregelen zijn niet zonder impact. De precieze maatschappelijke impact van deze kwetsbaarheid is op dit moment niet duidelijk. Deze wordt op dit moment onderzocht en nauwgezet gevolgd.
- Gistermiddag is er een patch beschikbaar gekomen. Het NCSC adviseert partijen om, totdat de kwetsbaarheden verholpen zijn, een risicoafweging te maken per systeem dat PHP gebruikt en aan het internet hangt of aanvullende maatregelen noodzakelijk zijn, zoals het uitschakelen van het systeem. Dit advies geldt ook voor Rijksoverheidsorganisaties.
- Daarnaast laat dit nogmaals zien dat het van belang is om de basismaatregelen die het NCSC adviseert op orde te hebben. Verder blijft het nodig om onze cyberweerbaarheid permanent te versterken, in dit kader wordt de Kamer op korte termijn geïnformeerd over een actieprogramma.

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Cybersecurity en Statelijke dreigingen
Cybersecurity

Datum
22 oktober 2026

4. Toelichting

n.v.t.

5. Informatie die niet openbaar gemaakt kan worden

5.1. Toelichting

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.