

ISS GLOBAL / INCIDENTONDERZOEK



PHP-beveiligingswaarschuwing: grootschalige tijdelijke sluiting van websites

Preventieve opschorting van diensten gemeld op 21 oktober 2026

VERSLAG- / ONDERZOEKSPERIODE

21 oktober 2026, 00:00–23:59 Europe/London. Voorafgaande waarschuwing van 20 oktober als context; bronnen geraadpleegd op 22 oktober.

UITGAVEDATUM

2026-10-22

Officiële berichten bevestigen dat meerdere beheerders onlinediensten buiten gebruik stelden als reactie op kritieke PHP-kwetsbaarheden. Het bewijs ondersteunt een grootschalige preventieve verstoring; het toont niet aan dat elke onbereikbare website was gecompromitteerd.

Kernbeoordeling

Een gedeelde softwareafhankelijkheid maakte dringend herstel noodzakelijk bij verder los van elkaar staande organisaties. Besluiten van beheerders om diensten te isoleren verklaren de gedocumenteerde gevallen. Een storing, een kwetsbaar systeem en een bevestigde inbraak moeten afzonderlijk worden geregistreerd. ^[4] ^[6] ^[7]

In dit rapport

Reconstructie; technische oorzaak; tijdlijn van waarschuwingen en patches; bevestigde gevolgen voor diensten; toetsing van bewijs en attributie; verificatie van herstel; openstaande vragen en tien gekoppelde primaire bronnen.

Uitgave opgesteld op 22 oktober 2026. Beoordeling op basis van openbare bronnen; geen interne systeemlogs of forensische bewijsstukken onderzocht.

Nederlandse vertaling, gecontroleerd aan de hand van de Engelse editie. Technische termen en verificatiemethode staan in het vertaalverantwoordingsblad.

Van beveiligingswaarschuwing naar dienstverstoring

Aanleiding

Het PHP-project kondigde op 20 oktober een spoedrelease met beveiligingsupdates aan, gepland voor de volgende dag om 14:00 UTC. Het advies van 21 oktober beschrijft twee kritieke kwetsbaarheden die remote code execution zonder authenticatie mogelijk maken. Het gaat om een gedeelde softwarekwetsbaarheid in systemen die PHP gebruiken om webrequests af te handelen. ^[1]

Reactie van beheerders

De Nederlandse overheid bevestigt dat onder meer Overheid.nl, MijnOverheid.nl en DigiD op 21 oktober uit voorzorg offline zijn gehaald. Zij meldt ook dat veel overheidswebsites, waaronder Rijksoverheid.nl, geen PHP gebruiken en niet door deze kwetsbaarheid werden geraakt. ^[4]

ASIMUT verklaart dat de toegang werd opgeschort in afwachting van het toepassen en verifiëren van beveiligingsupdates. Georgetown University meldt dat getroffen servers onmiddellijk offline werden gehaald om updates te installeren, met de waarschuwing dat universitaire websites en diensten tijdelijk onbereikbaar konden zijn. Dit zijn afzonderlijke beheerders die hun eigen maatregelen beschrijven. ^{[6] [7]}

Beoordeling door ISS Global

De best onderbouwde verklaring voor deze voorbeelden is het uit voorzorg buiten gebruik stellen van diensten terwijl een dringende reparatie werd voorbereid en uitgerold. Gebruikers ondervonden onbereikbaarheid, maar dat verschijnsel alleen bewijst geen cyberaanval. Een gedeelde kwetsbaarheid verklaart waarom onafhankelijke organisaties binnen dezelfde verslagperiode vergelijkbare besluiten konden nemen.

Het onderzochte bewijs toont een verstoring bij meerdere organisaties aan. Het bewijst geen enkele storing van het gehele internet, geen volledige lijst van getroffen websites en geen gezamenlijk begin- en eindtijdstip. Voor dergelijke verdergaande conclusies zijn een afgebakende meetpopulatie en dienstregistraties met tijdstempels nodig.

Betekenis van de kwetsbaarheden

IDENTIFICATIE	UITLEG VAN DE LEVERANCIER	OPERATIONELE BETEKENIS
CVE-2026-109618	Out-of-memory-afhandeling kan requestgegevens onvolledig geïnitieerd achterlaten.	Verdere verwerking kan leiden tot memory corruption en remote code execution. [1]
CVE-2026-109619	Interne requeststatus kan blijven bestaan nadat het bijbehorende geheugen is vrijgegeven.	Een latere request kan verouderde status (stale state) aantreffen, waardoor remote code execution mogelijk wordt. [1]

Bron van de leverancier: [1]

PHP noemt 8.5.12, 8.4.27, 8.3.36 en 8.2.35 als versies waarin de fouten zijn verholpen. Volgens het project lopen alle installaties die webrequests afhandelen risico; Apache mod_php geldt in die beoordeling als de configuratie met het hoogste risico. De inrichting van de omgeving is bepalend: blootstelling betekent niet dat elke configuratie even goed misbruikbaar is. [1]

Waarom inloggen geen afdoende grens vormde

Het Britse NCSC waarschuwt dat de kwetsbaarheid onder bepaalde omstandigheden uitvoering zonder authenticatie mogelijk maakt. Het adviseert PHP in de gehele infrastructuur te inventariseren, publiek toegankelijke systemen voorrang te geven, leveranciersupdates toe te passen en te overwegen systemen offline te halen als updates en tijdelijke maatregelen niet tijdig kunnen worden doorgevoerd. [2]

Meer dan openbare webpagina's

Het Zwitserse NCSC neemt ook interne applicaties, beheerinterfaces, hostingplatforms, containers en appliances op in de inventarisatie. Het wijst erop dat een leverancier fixes kan backporten zonder het hoofdversienummer te wijzigen. Daarom zijn de exacte packageversie en de beveiligingsinformatie van de leverancier van belang. [8]

Duiding door ISS Global

Een pagina kan statisch lijken terwijl de achterliggende dienst een kwetsbare component gebruikt. Omgekeerd is een website zonder PHP niet aantoonbaar getroffen alleen omdat PHP elders veel wordt gebruikt. De beoordeling moet uitgaan van de uitgerolde applicatie en haar werkelijke afhankelijkheden.

03 / TIJDLIJN

Waarschuwing, opschorting en patching

DATUM / TIJD	GEDOCUMENTEERDE ONTWIKKELING	DUIDING
20 oktober	PHP kondigt een kritieke release vooraf aan. [1]	Voorbereidingstijd; geen algemeen begin van de storing.
21 oktober, vóór de release	ASIMUT meldt opschorting in afwachting van updates. [6]	Rechtstreekse verklaring over preventief handelen.
21 oktober, 13:30 UTC / 14:30 BST	CERT-EU meldt dat fixes om 13:30 UTC zijn uitgebracht. [3]	Aan CERT-EU toegeschreven relesetijd; eerder dan gepland.
21 oktober, 15:13 CEST / 14:13 BST	Overheidsbericht noemt opgeschorte diensten. [4]	Publicatietijd; niet het tijdstip waarop elke dienst offline ging.
21 oktober, 15:50 CEST / 14:50 BST	NCSC-community meldt beschikbare patches. [5]	Tijdstip van berichtgeving; geen alternatieve relesetijd.
21 oktober, 20:40 CEST / 19:40 BST	NCSC meldt dat de hoofdwebsite weer bereikbaar is. [5]	Ondersteunt herstel van die website; zegt niets over andere diensten.

Bronnen bij de tijdlijn: [1] [3] [4] [5] [6]

Controle van tijdsaanduidingen

De release was gepland voor 14:00 UTC, gelijk aan 15:00 BST en 16:00 CEST. CERT-EU noemt een eerder werkelijk tijdstip. ASIMUT raamde herstel op ongeveer 45 minuten na de verwachte release, mits uitrol en verificatie slaagden. Die raming wordt niet als waargenomen hersteltijd gebruikt. [3] [6]

De overheidspagina bevat nog tekst van vóór de release naast een update zonder tijdsaanduiding dat patches beschikbaar zijn. Deze veranderende berichten moeten als opeenvolgende communicatie worden gelezen, niet als bewijs dat de patch op elk genoemd tijdstip nog ontbrak. [4]

Uit deze berichten kan geen volledige uitvalduur per dienst worden berekend. Een publicatietijd van een prognose aftrekken zou een niet-onderbouwde duur opleveren.

Welke diensten werden geraakt?

ORGANISATIE / DIENST	WAT DE OORSPRONKELIJKE BRON ONDERBOUWT	WAT ONBEKEND BLIJFT
Nederlandse overheidsdiensten	Preventieve opschorting van genoemde publieke portalen. [4]	Exacte duur, aantal gebruikers en transactieachterstand.
NCSC Nederland	Eigen hoofdwebsite tijdelijk offline; community voor updates, later herstel gemeld. [5]	Exact moment van opschorting en volledige resultaten van hersteltests.
ASIMUT	Toegang tijdelijk opgeschort in afwachting van updates en verificatie. [6]	Waargenomen hersteltijd en aantal getroffen gebruikers.
Georgetown University	Getroffen servers offline voor patching; mogelijke uitval van websites en diensten. [7]	Specifieke lijst van diensten en tijdstip van volledig herstel.

Rechtstreekse verklaringen: [4] [5] [6] [7]

Gevolgen: beoordeling door ISS Global

Onbereikbaarheid van publieke portalen kan gebruikers beletten een handeling af te ronden, ook als gegevens intact blijven. Plannings- en onderwijssystemen stellen andere eisen aan continuïteit, zoals alternatieve toegang, omgang met deadlines en communicatie met gebruikers. Dit zijn aannemelijke operationele gevolgen; de bronnen kwantificeren geen verloren transacties of gemiste activiteiten.

Beperkingen bij het bepalen van de omvang

Dit is een gedocumenteerde selectie van gevallen, geen volledige inventarisatie. Zij omvat openbaar bestuur, commerciële software en hoger onderwijs. Het aantal PHP-afhankelijke websites is niet gelijk aan het aantal offline gehaalde websites; geen van beide aantallen is een telling van gecompromitteerde systemen.

Waarschuwing van een autoriteit versus storingsbewijs

NHS England publiceerde een waarschuwing met hoge ernst en achtte toekomstig misbruik zeer waarschijnlijk. Dat onderbouwt een waarschuwing voor de zorgsector, geen NHS-storing. Drupal legt de verantwoordelijkheid voor platformonderhoud bij eigenaren en hostingpartijen; het bericht bewijst niet dat Drupal.org onbereikbaar was. [9] [10]

Voor deze selectie zijn geen schaderaming, bevestigde gegevensdiefstal, slachtoffers of geïdentificeerde kwaadwillende partij vastgesteld.

Blootstelling, aanval en compromittering

VRAAG	BEWIJS BIJ AFSLUITING VAN DE VERSLAGPERIODE	ZEKERHEID / VOORBEHOUD
Waren er ernstige kwetsbaarheden?	Advies van de ontwikkelaar en herstelde releases. [1]	Hoog: oorspronkelijke leveranciersinformatie.
Zijn diensten bewust buiten gebruik gesteld?	Rechtstreekse verklaringen van beheerders en overheid. [4,6,7]	Hoog voor die verklaringen; geen onafhankelijke uptimedataset onderzocht.
Was misbruik technisch mogelijk?	NHS-waarschuwing meldt geslaagde demonstraties door onderzoekers. [10]	Gedocumenteerde berichtgeving; geen telling van werkelijk getroffen organisaties.
Was kwaadwillig misbruik bevestigd?	Eerste Nederlandse bericht meldt geen waargenomen actief misbruik; CERT-EU waarschuwt voor grotere waarschijnlijkheid. [3,5]	Verschillende momenten en bewijscategorieën; hier geen bewijs van een getroffen organisatie.
Wie veroorzaakte de verstoring?	Genoemde beheerders beschrijven preventieve besluiten.	Geen onderbouwde toeschrijving van deze opschortingen aan een kwaadwillende partij.

Bronnen voor de toetsing: [1] [3] [4] [5] [6] [7] [10]

De schijnbare tegenstelling

De mededeling dat een autoriteit geen actief misbruik heeft waargenomen, is begrensd door haar zicht op de situatie en het moment van waarneming. Een verwachting dat misbruik waarschijnlijk is, is een risicobeoordeling. Geen van beide bewijst algemene veiligheid of bevestigt een inbraak bij een specifieke dienst. Het rapport behoudt beide uitspraken met hun oorspronkelijke bewijsstatus.

Onafhankelijkheid van bronnen

PHP is de oorspronkelijke bron voor de kwetsbaarheid en de reparatie. Beveiligingsautoriteiten duiden grotendeels dezelfde technische bevinding; herhaling vormt geen onafhankelijke ontdekking van tien afzonderlijke fouten. Berichten van beheerders onderbouwen wel onafhankelijk verschillende besluiten om diensten buiten gebruik te stellen.

Niet onderzocht

Serverlogs, forensische systeemimages voor incident response, wijzigingsregistraties van providers en onafhankelijke beschikbaarheidsmetingen van getroffen organisaties waren niet beschikbaar. Voor het vaststellen van een preventieve opschorting waren geen geauthenticeerde incidentbeelden nodig. Er is geen geografische kaart opgenomen: de registraties meten geen fysieke verspreiding die daarop verantwoord kan worden weergegeven.

Wat aantoonbaar herstel moet onderbouwen

Gepubliceerde richtlijnen

Drupal adviseert eigenaren die PHP zelf beheren om het te updaten; gebruikers van managed hosting moeten de communicatie van hun hostingpartij volgen. Volgens het bericht biedt een PHP-release met de fix een volledige oplossing voor de kwetsbaarheid. Eigenaren en leveranciers blijven verantwoordelijk voor onderhoud van het platform en componenten van derden. ^[9]

Het Zwitserse NCSC adviseert na updates getroffen diensten en langlopende processen te herstarten, te controleren of de actieve applicatie een hersteld package gebruikt en op afwijkingen te onderzoeken. Het benadrukt dat een update een al opgetreden compromittering niet ongedaan maakt. Tijdelijke maatregelen beperken specifieke aanvalspaden en vervangen patching niet. ^[8]

Voorgesteld verificatiedossier: ISS Global

1. **Afbakening:** leg de dienst, eigenaar, PHP-afhankelijkheid, uitgerolde omgeving en leverancier vast, inclusief extern beheerde componenten.
2. **Inperking:** registreer wanneer toegang werd beperkt, waarom, welke uitzonderingen waren goedgekeurd en welk alternatief gebruikers kregen.
3. **Reparatie:** bewaar per instance het leveranciersadvies, de identificatie van het herstelde package en de uitrolregistratie.
4. **Runtime-verificatie:** bevestig dat actieve diensten de herstelde build gebruiken; vertrouw niet uitsluitend op een lijst van geïnstalleerde packages.
5. **Herstel:** controleer essentiële gebruikershandelingen en ondersteunende diensten voordat herstel wordt geregistreerd.
6. **Beveiligingscontrole:** bewaar bewijs van verdachte activiteit en volg het onderzoek afzonderlijk van het herstel van de beschikbaarheid.

Rapportage aan het management

Een verificatieverklaring moet aangeven welke diensten zijn gecontroleerd en wat nog openstaat. “Website weer online” beantwoordt een vraag over beschikbaarheid; het bewijst niet dat elke afhankelijkheid is hersteld of dat eerdere compromittering is uitgesloten.

Dit onderzoek beoordeelt niet de blootstelling van de eigen website van ISS Global. Daarvoor is een afzonderlijke beoordeling van hosting en uitgerolde afhankelijkheden nodig; dit rapport betreft het bredere openbare incident.

Beoordeling aan het einde van 21 oktober

Hoofdbevinding

ISS Global beoordeelt de gedocumenteerde opschortingen als een preventieve beperking van de beschikbaarheid als gevolg van een ernstige gedeelde softwarekwetsbaarheid. Onafhankelijke verklaringen van beheerders ondersteunen die uitleg. Het dossier rechtvaardigt niet dat alle getroffen diensten als gehackt worden beschreven of dat het incident aan één kwaadwillende partij wordt toegeschreven.

Resterend risico

De verwachting van NHS England dat misbruik waarschijnlijk is, onderstreept de noodzaak van snel herstel. Een ernstscore is echter geen kansberekening voor compromittering van een specifieke installatie. Blootstelling moet worden beoordeeld op basis van de werkelijke inrichting; beveiligingsconclusies vereisen lokaal bewijs. ^[10]

Openstaande vragen met voorrang

- Welke andere beheerders stelden daadwerkelijk diensten buiten gebruik, in plaats van alleen een advies te publiceren?
- Wat waren de geverifieerde begin- en hersteltijden per dienst?
- Welk hersteld package draaide bij heropening op elke getroffen instance?
- Is kwaadwillige activiteit waargenomen en gekoppeld aan een van beide kwetsbaarheden?
- Welke gevolgen voor gebruikers bleven na herstel bestaan, zoals werk in wachtrijen en mislukte transacties?

Afbakening en beperkingen

Onderwerp: grootschalige PHP-gerelateerde opschortingen gemeld op 21 oktober 2026, door de opdrachtgever bevestigd. Verslagperiode: die volledige kalenderdag in Europe/London, met de voorafgaande waarschuwing van 20 oktober als context. Bronnen zijn geraadpleegd op 22 oktober. Doorlopend bijgewerkte pagina's kunnen wijzigingen zonder tijdstempel bevatten; er was geen historische momentopname om elke zin op het afsluitmoment te verifiëren. Geen uitkomst met een latere datum is verwerkt.

Nederlandstalige oorspronkelijke bronnen zijn voor de Engelse editie gelezen en vertaald. Tien primaire bronregistraties ondersteunen het rapport. De selectie toont spreiding zonder volledigheid te claimen. Er zijn geen geografische incidentiecijfers, wereldwijd storingsaantal of financiële totaalschade berekend.

Controle op eerdere uitgaven: mailboxresultaten toonden een rapport van 21 oktober met de titel "UK infrastructure outages and possible links". De volledige inhoud is niet onderzocht; inhoudelijke overlap is dus niet uit te sluiten. Er is geen eerdere PHP-specifieke uitgave vastgesteld; controle van het volledige archief blijft onvolledig.

Oorspronkelijk opgesteld als nieuw onderzoek naar een aangewezen incident. De Engelse editie is daarna aan de vier bevestigde ontvangers verzonden. Voor deze Nederlandse editie is geen e-maildistributie gevraagd.

Terminologie en verificatie

Deze Nederlandse editie is vertaald uit de definitieve Engelse editie van 22 oktober 2026. De tekst is per onderdeel vergeleken op betekenis, volledigheid, bronverwijzingen, ontkenningen, onzekerheden, datums en getallen. Dit is een door de assistent uitgevoerde vertaling met een afzonderlijke controlepass; geen beëdigde vertaling of onafhankelijke menselijke revisie.

TERM / CATEGORIE	KEUZE IN DEZE EDITIE
PHP; CVE-2026-109618; CVE-2026-109619	Ongewijzigd; hetzelfde geldt voor versie- en adviesnummers.
remote code execution (RCE)	Engelse vakterm behouden; “zonder authenticatie” vertaalt unauthenticated.
out-of-memory; memory corruption; stale state	Vaktermen behouden, met Nederlandse uitleg waar nodig.
Apache mod_php; Drupal; ASIMUT; DigiD	Product-, configuratie- en dienstnamen ongewijzigd.
patch; patching; runtime; build; package; instance	Gangbare technische termen behouden; geen betekenisveranderende letterlijke vertaling.
compromise / compromised	Compromittering / gecompromitteerd: aantasting van een systeem, niet een zakelijk compromis.
incident-response images	Forensische systeemimages voor incident response; niet vertaald als gewone foto's.
UTC; BST; CEST; Europe/ London	Ongewijzigd; tijden en onderlinge omzettingen uit het origineel behouden.

Controle-uitkomst

CVE-identificaties, softwareversies, tijden, de raming van 45 minuten, tien bron-URL's en bronnummering zijn met het origineel vergeleken. De bewijsstatus blijft onderscheiden: een voorzorgsmaatregel is geen bevestigde aanval; een prognose is geen waargenomen hersteltijd; een waarschuwing bewijst geen storing bij de uitgevende autoriteit.

Oorspronkelijke brontitels en officiële organisatienamen blijven behouden om terugzoeken te vergemakkelijken. Bronbeschrijvingen en toegangsbeperkingen zijn vertaald. De enige inhoudelijke actualisering betreft de distributiestatus van de Engelse editie; dit verandert geen incidentbevinding.

BRONNENREGISTER

Bronnen 01–05

Hieronder staan bronfamilies en toegangsbeperkingen. Herhaling van een verklaring vormt geen onafhankelijk bewijs.

-
- 01 **News Archive 2026: advance notice, security advisory and fixed releases**
PHP project · 20 en 21 oktober 2026
Bronfamilie: Softwareontwikkelaar / oorspronkelijke release · Geraadpleegd op 22 oktober 2026. Volledige relevante berichten; Engels. Doorlopend bijgewerkt archief; oorspronkelijke publicatietijden ontbreken. Technische oorzaak en herstelde versies zijn bevindingen van de leverancier.
<https://www.php.net/archive/2026.php>
-
- 02 **Critical security issue affecting PHP**
UK National Cyber Security Centre · 21 oktober 2026
Bronfamilie: Britse autoriteit / op leveranciersinformatie gebaseerd advies · Geraadpleegd op 22 oktober 2026. Volledige waarschuwing; Engels. Geraadpleegde versie bevat advies van na de release; geen afzonderlijk update-tijdstip.
<https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php>
-
- 03 **Security Advisory 2026-018: Critical Vulnerabilities in PHP**
CERT-EU · 21 oktober 2026; v1.0 en v1.1 op dezelfde datum; weergegeven release 15:20:18, tijdzone niet vermeld
Bronfamilie: Beveiliging EU-instellingen / op leveranciersinformatie gebaseerd advies · Geraadpleegd op 22 oktober 2026. Volledig advies; Engels. Releasetijd toegeschreven aan CERT-EU; waarschijnlijkheid van misbruik is een beoordeling, geen vaststelling bij een getroffen organisatie.
<https://cert.europa.eu/publications/security-advisories/2026-018/>
-
- 04 **Aantal websites Rijksoverheid preventief offline na kwetsbaarheden PHP**
Government of the Netherlands · 21 oktober 2026, 15:13 lokale tijd weergegeven; update zonder tijdstip
Bronfamilie: Overheidsbericht over gevolgen voor diensten · Geraadpleegd op 22 oktober 2026. Volledige Nederlandse pagina; voor de Engelse editie vertaald door ISS Global. Bevestigt genoemde preventieve opschortingen; geen exacte begin- en eindtijden. Doorlopend bijgewerkt.
<https://www.rijksoverheid.nl/actueel/nieuws/2026/10/21/aantal-websites-rijksoverheid-preventief-offline-na-kwetsbaarheden-php>
-
- 05 **Blijf op de hoogte van de PHP-kwetsbaarheden**
NCSC Netherlands · 21 oktober 2026, 11:03; updates 14:30, 15:50 en 20:40 weergegeven
Bronfamilie: Nederlandse autoriteit / status van eigen dienst · Geraadpleegd op 22 oktober 2026. Volledig Nederlands communitybericht; voor de Engelse editie vertaald door ISS Global. Latere updatekoppen herhalen de datum niet; gelezen binnen de gedateerde incidentcontext.
<https://community.ncsc.nl/p/php>
-

BRONNENREGISTER

Bronnen 06–10

Hieronder staan bronfamilies en toegangsbeperkingen. Herhaling van een verklaring vormt geen onafhankelijk bewijs.

-
- 06 Temporary service interruption
ASIMUT / Dennis Jung Møller · 21 oktober 2026; metadata 14:53:36 +02:00
Bronfamilie: Onafhankelijke beheerder / rechtstreekse verklaring over opschorting · Geraadpleegd op 22 oktober 2026. Volledig Engels bericht. Herstelraming is voorwaardelijk; geen bevestiging van herstel of exacte uitvalduur.
<https://asimut.com/news/temporary-service-interruption/>
-
- 07 Service Notice: Potential Website Outages Due to Critical PHP Vulnerabilities
Georgetown University Information Services · 21 oktober 2026
Bronfamilie: Onafhankelijke universitaire beheerder / rechtstreekse responsverklaring · Geraadpleegd op 22 oktober 2026. Volledig Engels bericht. Bevestigt isolatie van getroffen servers; mogelijke dienstgevolgen; geen lijst of tijdstip van afronding.
<https://uis.georgetown.edu/uis-announcement/service-notice-potential-website-outages-due-to-critical-php-vulnerabilities/>
-
- 08 Critical vulnerabilities in PHP: Install security updates immediately
Swiss National Cyber Security Centre · 21 oktober 2026
Bronfamilie: Zwitserse autoriteit / op leveranciersinformatie gebaseerd advies · Geraadpleegd op 22 oktober 2026. Volledige officiële Engelse pagina. Advies en verificatierichtlijnen; geen bewijs van uitval van een Zwitserse dienst.
<https://www.bacs.admin.ch/en/warnung-php-en>
-
- 09 Critical PHP update on Wednesday, October 21, 2026 (14:00 UTC) - PSA-2026-10-20
Drupal Security Team · Weergegeven datum 21 oktober 2026; identificatiecode bevat 20 oktober
Bronfamilie: Applicatie-ecosysteem / verantwoordelijkheid hosting · Geraadpleegd op 22 oktober 2026. Volledig Engels bericht. Datering op basis van weergegeven datum, niet de identificatiecode. Bevestigt geen storing van Drupal.org.
<https://www.drupal.org/psa-2026-10-20>
-
- 10 Critical Vulnerabilities in PHP (PHP2Shell), CC-4875
NHS England Digital · 21 oktober 2026, 15:51 weergegeven; laatst bijgewerkt op hetzelfde tijdstip
Bronfamilie: Beveiligingsautoriteit zorgsector / dreigingsbeoordeling · Geraadpleegd op 22 oktober 2026. Volledige Engelse waarschuwing. Aangevoerd technisch misbruik en verwacht risico zijn onderscheiden van een bevestigde NHS-compromittering of -storing.
<https://digital.nhs.uk/cyber-alerts/2026/cc-4875>
-