Raad van de Europese Unie

Brussel, 17 december 2025
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	11 december 2025
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	C(2025) 8407 final
Betreft:	GEDELEGEERDE VERORDENING (EU) …/... VAN DE COMMISSIE van 11.12.2025 tot aanvulling van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad door de voorwaarden te specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen voor het uitstellen van de verspreiding van meldingen

De delegaties vinden hierbij document C(2025) 8407 final.

Bijlage: C(2025) 8407 final

EUROPESE
COMMISSIE

Brussel, 11.12.2025
C(2025) 8407 final

GEDELEGEERDE VERORDENING (EU) …/... VAN DE COMMISSIE

van 11.12.2025

tot aanvulling van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad door de voorwaarden te specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen voor het uitstellen van de verspreiding van meldingen

(Voor de EER relevante tekst)

TOELICHTING

1. ACHTERGROND VAN DE GEDELEGEERDE HANDELING

Op grond van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad ("verordening cyberweerbaarheid") moeten fabrikanten van producten met digitale elementen via een centraal meldingsplatform melding maken van elke actief uitgebuite kwetsbaarheid of elk ernstig incident dat gevolgen heeft voor de beveiliging van een product met digitale elementen. Op grond van artikel 16, lid 2, van die verordening kan het door de lidstaat als coördinator aangewezen computer security incident response team (CSIRT) dat als eerste de melding ontvangt, in uitzonderlijke omstandigheden en op basis van gegronde cyberbeveiligingsgerelateerde redenen de verspreiding van de melding naar de CSIRT's van andere lidstaten waar het product met digitale elementen beschikbaar is gesteld, uitstellen.

Deze gedelegeerde handeling is dan ook bedoeld om de verordening cyberweerbaarheid aan te vullen door de voorwaarden te specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen om de verspreiding van meldingen uit te stellen. Daartoe worden drie soorten redenen genoemd waarom het CSIRT dat als eerste de melding ontvangt, kan besluiten dat het noodzakelijk is de verdere verspreiding naar andere CSIRT's uit te stellen. Een dergelijk besluit tot uitstel kan in drie gevallen worden genomen:

- in het licht van een beoordeling van de aard van de gemelde informatie;
- indien het CSIRT dat de melding ontvangt, niet in staat is de vertrouwelijkheid van dergelijke informatie te waarborgen;
- indien het centrale meldingsplatform is gecompromitteerd of tijdelijk niet operationeel is.

De rapportageverplichtingen van artikel 14 van Verordening (EU) 2024/2847 zijn van toepassing met ingang van 11 september 2026.

2. RAADPLEGINGEN VOORAFGAAND AAN DE VASTSTELLING VAN DE HANDELING

Het CSIRT-netwerk en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) zijn geraadpleegd over verschillende ontwerpen van deze handeling. Op 26 maart 2025 vond een voorbereidende bespreking met oriënterende vragen plaats, waarna uiterlijk op 11 april 2025 nog schriftelijke input kon worden geleverd. Een eerste ontwerp van deze handeling werd op 16 mei 2025 gedeeld met het CSIRT-netwerk en Enisa en op 6 juni 2025 besproken, waarna uiterlijk op 27 juni 2025 nog schriftelijke input kon worden geleverd. Een tweede ontwerp van deze handeling werd op 23 juli 2025 gedeeld met het CSIRT-netwerk en Enisa, waarna uiterlijk op 1 september 2025 nog schriftelijke input kon worden geleverd. Een derde ontwerp van deze handeling werd op 25 september 2025 gedeeld met het CSIRT-netwerk en Enisa en op 9 oktober 2025 besproken, waarna uiterlijk op 27 oktober 2025 nog schriftelijke input kon worden geleverd.

Tussen 16 oktober 2025 en 13 november 2025 is over de ontwerphandeling een openbare raadpleging gehouden, waarop 34 antwoorden van 31 unieke respondenten zijn ontvangen (éénzelfde respondent diende vier keer feedback in). Hiervan was 29,41 % afkomstig van bedrijfsverenigingen, 26,47 % van bedrijven/ondernemingen, 17,65 % van EU-burgers,

14,71 % van overheidsinstanties, 5,88 % van niet-gouvernementele organisaties (ngo's) en 5,88 % van academische/onderzoeksinstellingen[1].

Op 22 oktober werd het ontwerp ook besproken met de deskundigengroep voor de cyberbeveiliging van producten met digitale elementen (E03967), waarvan de autoriteiten van de lidstaten, Enisa, op persoonlijke titel benoemde individuele deskundigen en organisaties in de brede zin van het woord (bv. bedrijven, verenigingen, ngo's) lid zijn.

3. JURIDISCHE ELEMENTEN VAN DE GEDELEGEERDE HANDELING

De bevoegdheid om gedelegeerde handelingen vast te stellen is vastgelegd in artikel 14, lid 9, van de verordening cyberweerbaarheid, op grond waarvan de Commissie uiterlijk op 11 december 2025 de voorwaarden moet specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen voor het uitstellen van de verspreiding van meldingen.

[1] Deze percentages houden geen rekening met het feit dat dezelfde respondent vier keer feedback heeft ingediend.

GEDELEGEERDE VERORDENING (EU) …/... VAN DE COMMISSIE

van 11.12.2025

tot aanvulling van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad door de voorwaarden te specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen voor het uitstellen van de verspreiding van meldingen

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid)[2], en met name artikel 14, lid 9,

Overwegende hetgeen volgt:

(1) In uitzonderlijke omstandigheden, en met name op verzoek van de fabrikant en in het licht van het gevoeligheidsniveau van de gemelde informatie, en op basis van gegronde cyberbeveiligingsgerelateerde redenen, kan het als coördinator aangewezen computer security incident response team (CSIRT) dat als eerste een melding ontvangt van een actief uitgebuite kwetsbaarheid of een ernstig incident dat gevolgen heeft voor de beveiliging van een product met digitale elementen (“het CSIRT dat als eerste de melding ontvangt”), besluiten tot uitstel - voor een periode die niet langer is dan strikt noodzakelijk - van de verspreiding van de melding via het centrale meldingsplatform naar de CSIRT’s die als coördinatoren zijn aangewezen op het grondgebied waarvan de fabrikant die de melding indient, heeft aangegeven dat het product met digitale elementen beschikbaar is gesteld (“de betrokken CSIRT’s”). Daarom moeten de voorwaarden voor de toepassing van dergelijke redenen worden vastgesteld. Wanneer dergelijke redenen van toepassing zijn, mag het CSIRT dat als eerste de melding ontvangt, de verspreiding naar de betrokken CSIRT’s uitstellen voor een periode die niet langer is dan strikt noodzakelijk, maar is daartoe niet verplicht. Volgens artikel 16, lid 2, van Verordening (EU) 2024/2847 moet een CSIRT dat als eerste de melding ontvangt en besluit zich op dergelijke redenen te beroepen, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) onmiddellijk in kennis stellen van zijn besluit om de melding uit te stellen en van de redenen daarvoor, en wanneer het voornemens is de melding te verspreiden.

(2) Overeenkomstig artikel 16, lid 2, tweede alinea, van Verordening (EU) 2024/2847 zijn de algemene voorwaarden voor de toepassing van de in deze verordening uiteengezette cyberbeveiligingsgerelateerde redenen niet van toepassing op de toegang van Enisa tot de gemelde informatie. De toegang van Enisa tot de gemelde informatie mag alleen in bijzonder uitzonderlijke omstandigheden worden beperkt: wanneer de fabrikant in zijn

[2] PB L 2024/2847 van 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

melding aangeeft dat aan een van de drie voorwaarden van artikel 16, lid 2, derde alinea, punt a), b) of c), van Verordening (EU) 2024/2847 is voldaan, en dan alleen met betrekking tot de kwetsbaarheidsmelding binnen 72 uur als bedoeld in artikel 14, lid 2, punt b), van Verordening (EU) 2024/2847. In dergelijke gevallen is de enige informatie die tegelijkertijd aan Enisa ter beschikking moet worden gesteld, informatie dat een fabrikant een melding heeft gedaan; algemene informatie over het product met digitale elementen; informatie over de algemene aard van de uitbuiting; en de informatie dat beveiligingsgerelateerde redenen zijn ingeroepen.

(3) Toegang tot de gemelde informatie stelt CSIRT's in staat een overzicht te krijgen van de beveiligingsomgeving op hun grondgebied en risicobeperkende maatregelen te nemen, waardoor het algemene cyberbeveiligingsniveau in de Unie wordt verhoogd. Daarom mogen verdere beperkingen op de verspreiding van meldingen in het licht van de aard van de informatie waarvan melding wordt gedaan, alleen mogelijk zijn in gevallen waarin, gezien de gevoeligheid van de gemelde informatie, de cyberbeveiligingsrisico's die voortvloeien uit verdere verspreiding groter zijn dan de beveiligingsvoordelen voor de Unie, en die risico's niet adequaat kunnen worden beperkt door beperkingen op te leggen aan de respons op en verdere verspreiding van de melding via passende protocollen die binnen het CSIRT-netwerk worden gebruikt, zoals het *Traffic Light Protocol* (TLP) of het *Permissible Actions Protocol* (PAP). Dit kan bijvoorbeeld het geval zijn wanneer een fabrikant het CSIRT dat als eerste de melding ontvangt, heeft meegedeeld dat hij binnenkort een risicobeperkende maatregel (zoals een patch) verwacht te verstrekken. Dit kan ook het geval zijn wanneer het CSIRT dat als eerste de melding ontvangt, besluit slechts delen van een melding te delen, en deze delen niettemin volstaan om de betrokken CSIRT's in staat te stellen passende risicobeperkende maatregelen te nemen. Voorts, en om samenwerking op het gebied van de identificatie en bekendmaking van kwetsbaarheden tussen fabrikanten, CSIRT's en beveiligingsonderzoekers aan te moedigen, kan dit ook het geval zijn wanneer het CSIRT optreedt als betrouwbare tussenpersoon voor een lopende procedure voor gecoördineerde bekendmaking van kwetsbaarheden als bedoeld in artikel 12, lid 1, van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[3]. In dat geval, wanneer het CSIRT besluit de verspreiding van een melding uit te stellen, moet dat CSIRT die melding overeenkomstig artikel 16, lid 6, van Verordening (EU) 2024/2847 uitstellen voor een periode die niet langer is dan strikt noodzakelijk en totdat de bij de procedure voor gecoördineerde bekendmaking van kwetsbaarheden betrokken partijen toestemming hebben gegeven voor openbaarmaking.

(4) De informatie in de melding zal de CSIRT's helpen hun taken in het kader van risicobeperking en incidentenbehandeling uit te voeren. In zeldzame gevallen kan dergelijke informatie echter volstaan om een techniek voor uitbuiting te creëren zonder aanvullend onderzoek, zelfs door actoren met beperkte vaardigheden en middelen. Indien kwaadwillige actoren toegang zouden krijgen tot die informatie, zou de cyberbeveiliging van de Unie zwaar worden getroffen, gezien het gemak waarmee de informatie kan worden uitgebuit. Dit kan bijvoorbeeld het geval zijn wanneer de kwetsbare versie van een stuk software slechts marginaal verschilt van eerdere, niet-

[3] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

kwetsbare versies. In dergelijke gevallen kan het CSIRT dat als eerste de melding ontvangt indien het van mening is dat de cyberbeveiligingsrisico's die voortvloeien uit verdere verspreiding niet adequaat kunnen worden beperkt door beperkingen op te leggen aan de verwerking en verdere uitwisseling, besluiten de verspreiding uit te stellen totdat een doeltreffende risicobeperkende maatregel, zoals een beveiligingsupdate of gebruikersrichtsnoeren, beschikbaar is.

(5) Indien een relevant CSIRT de gemelde informatie niet op adequate wijze kan beschermen, kunnen kwaadwillige actoren gevoelige informatie raadplegen en uitbuiten in de hele eengemaakte markt. Wanneer er ernstige bezorgdheid bestaat over het vermogen van een relevant CSIRT om de vertrouwelijkheid van de gemelde informatie te waarborgen, kan het CSIRT dat als eerste de melding ontvangt, daarom besluiten de verspreiding van een melding alleen naar dat relevante CSIRT uit te stellen totdat die bezorgdheid is weggenomen. Dit kan het geval zijn in situaties waarin een relevant CSIRT is getroffen door een cyberbeveiligingsincident dat zijn vermogen om veilig te functioneren aantast, of wanneer er bewijs of informatie is dat er aanzienlijke tekortkomingen in de capaciteiten van het CSIRT zijn vastgesteld, zoals ernstige beperkingen van de middelen die zijn vermogen om zijn functies uit te voeren in gevaar brengen, of het gebruik van verouderde of kwetsbare software.

(6) Om te voorkomen dat kwaadwillige actoren toegang krijgen tot gevoelige informatie, moet het CSIRT dat als eerste de melding ontvangt, wanneer het uit hoofde van artikel 16 van Verordening (EU) 2024/2847 opgerichte centrale meldingsplatform door een cyberbeveiligingsincident in gevaar is gebracht, de verspreiding via het centrale meldingsplatform uitstellen totdat het platform opnieuw in staat is de vertrouwelijkheid van de gemelde informatie te waarborgen.

(7) Overeenkomstig artikel 16, lid 2, eerste alinea, van Verordening (EU) 2024/2847 hoeft het CSIRT dat als eerste de melding ontvangt, geen melding te verspreiden naar enig ander relevant CSIRT indien de fabrikant aangeeft dat het product met digitale elementen alleen wordt aangeboden op de markt van de lidstaat van het CSIRT dat als eerste de melding ontvangt.

(8) De Commissie heeft bij het opstellen van het ontwerp van gedelegeerde handeling de relevante belanghebbenden geraadpleegd en om hun standpunten verzocht, en heeft de deskundigengroep voor de cyberbeveiliging van producten met digitale elementen geraadpleegd.

(9) Overeenkomstig artikel 14, lid 9, van Verordening (EU) 2024/2847 heeft de Commissie bij opstellen van het ontwerp van gedelegeerde handeling nauw samengewerkt met het op grond van artikel 15 van Richtlijn (EU) 2022/2555 opgerichte CSIRT-netwerk en Enisa,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

In deze verordening worden de voorwaarden vastgesteld voor de toepassing van de in artikel 16, lid 2, van Verordening (EU) 2024/2847 bedoelde cyberbeveiligingsgerelateerde redenen die het als coördinator aangewezen CSIRT dat als eerste de melding ontvangt overeenkomstig artikel 14, leden 1 en 3, en artikel 15, leden 1 en 2, van die verordening, in staat stellen de verspreiding van de melding naar de als coördinatoren aangewezen CSIRT's

op het grondgebied waarvan de fabrikant heeft aangegeven dat het product met digitale elementen beschikbaar is gesteld, uit te stellen.

Artikel 2

Definities

Voor de toepassing van deze verordening gelden de volgende definities:

(1) "CSIRT dat als eerste de melding ontvangt": het CSIRT dat is aangewezen als coördinator die als eerste de melding ontvangt overeenkomstig artikel 14, leden 1 en 3, en artikel 15, lieden 1 en 2, van Verordening (EU) 2024/2847;

(2) "relevant CSIRT": het als coördinator aangewezen CSIRT op het grondgebied waarvan de fabrikant heeft aangegeven dat het product met digitale elementen beschikbaar is gesteld.

Artikel 3

Voorwaarden voor de toepassing van cyberbeveiligingsgerelateerde redenen die voortvloeien uit de aard van de gerapporteerde informatie

Het CSIRT dat als eerste de melding ontvangt, kan besluiten de verspreiding van meldingen of delen daarvan naar de relevante CSIRT's voor een periode die niet langer is dan strikt noodzakelijk uit te stellen in gevallen waarin, gezien de gevoeligheid van de gemelde informatie, de cyberbeveiligingsrisico's van de verspreiding groter zijn dan de beveiligingsvoordelen ervan en die risico's niet kunnen worden beperkt door beperkingen op te leggen aan de behandeling of verdere verspreiding van de melding via passende protocollen, zoals het Traffic Light Protocol (TLP) of het Permissible Actions Protocol (PAP), en wanneer aan ten minste een van de volgende voorwaarden is voldaan:

(a) de fabrikant heeft het CSIRT dat als eerste de melding ontvangt, meegedeeld dat een doeltreffende risicobeperkende maatregel, zoals een beveiligingsupdate of gebruikersrichtsnoeren, naar verwachting binnen 72 uur beschikbaar zal worden gesteld; indien binnen deze termijn geen doeltreffende risicobeperkende maatregel beschikbaar wordt gesteld, verspreidt het CSIRT dat als eerste de melding ontvangt, de melding naar de relevante CSIRT's;

(b) de in de melding opgenomen informatie wordt, gezien de aard van de gemelde actief uitgebuite kwetsbaarheid, toereikend geacht om een techniek voor uitbuiting te creëren, met name wanneer de kwetsbaarheid gemakkelijk kan worden vastgesteld en uitgebuit door actoren met beperkte vaardigheden en middelen; zodra een doeltreffende risicobeperkende maatregel, zoals een beveiligingsupdate of gebruikersrichtsnoeren, beschikbaar is, verspreidt het CSIRT dat als eerste de melding ontvangt, de melding naar de relevante CSIRT's;

(c) het CSIRT dat als eerste de melding ontvangt, kan met de relevante CSIRT's voldoende informatie delen om ervoor te zorgen dat de relevante CSIRT's passende risicobeperkende maatregelen kunnen nemen; zodra een doeltreffende risicobeperkende maatregel, zoals een beveiligingsupdate of gebruikersrichtsnoeren, beschikbaar is, verspreidt het CSIRT dat als eerste de melding heeft ontvangen, de volledige melding naar de relevante CSIRT's;

(d) het CSIRT dat de melding van de actief uitgebuite kwetsbaarheid als eerste ontvangt, daarvan op de hoogte is gebracht in het kader van een gecoördineerde bekendmaking van kwetsbaarheden waarvoor dat CSIRT optreedt als betrouwbare tussenpersoon

overeenkomstig artikel 12, lid 1, van Richtlijn (EU) 2022/2555; in dat geval, en overeenkomstig artikel 16, lid 6, van Verordening (EU) 2024/2847, verspreidt het CSIRT dat als eerste de melding ontvangt, de melding naar de relevante CSIRT's wanneer uitstel niet langer strikt noodzakelijk is en de bij gecoördineerde bekendmaking van kwetsbaarheden betrokken partijen toestemming hebben gegeven voor de bekendmaking.

Artikel 4

Voorwaarden voor de toepassing van cyberbeveiligingsgerelateerde redenen met betrekking tot een specifiek CSIRT

Het CSIRT dat als eerste de melding ontvangt, kan besluiten de verspreiding van meldingen of delen daarvan naar een specifiek relevant CSIRT voor een periode die niet langer is dan strikt noodzakelijk uit te stellen in gevallen waarin:

(a) het relevante CSIRT is getroffen door een cyberbeveiligingsincident dat twijfel doet rijzen over zijn vermogen om de vertrouwelijkheid van de gemelde informatie te waarborgen;

(b) het voldoende redenen heeft om aan te nemen dat de capaciteiten van het relevante CSIRT ontoereikend zijn om de vertrouwelijkheid van de gemelde informatie te waarborgen.

In de in de eerste alinea, punt a), bedoelde gevallen kan het CSIRT dat als eerste de melding ontvangt, de verspreiding uitstellen totdat het relevante CSIRT het in artikel 15 van Richtlijn 2022/2555 bedoelde CSIRT-netwerk ervan in kennis heeft gesteld dat zijn vermogen om de vertrouwelijkheid van de meldingen te waarborgen, is hersteld.

In de in de eerste alinea, punt b), bedoelde gevallen kan het CSIRT dat als eerste de melding ontvangt, de verspreiding naar het relevante CSIRT uitstellen totdat dat CSIRT heeft aangetoond dat het de vastgestelde tekortkomingen heeft aangepakt.

Artikel 5

Voorwaarden voor de toepassing van cyberbeveiligingsgerelateerde redenen met betrekking tot het centrale meldingsplatform

Het CSIRT dat als eerste de melding ontvangt, kan besluiten de verspreiding van meldingen via het bij artikel 16 van Verordening (EU) 2024/2847 opgerichte centrale meldingsplatform uit te stellen wanneer Enisa het CSIRT-netwerk overeenkomstig artikel 16, lid 4, van die verordening ervan in kennis heeft gesteld dat het centrale meldingsplatform is getroffen door een cyberbeveiligingsincident dat twijfel doet rijzen over zijn vermogen om de vertrouwelijkheid van de gemelde informatie te waarborgen. In dergelijke gevallen kan het CSIRT dat als eerste de melding ontvangt, de verspreiding via het centrale meldingsplatform uitstellen totdat Enisa het CSIRT-netwerk ervan in kennis heeft gesteld dat het platform opnieuw in staat is de vertrouwelijkheid van de meldingen te waarborgen.

Artikel 6

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 11.12.2025

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN