Europeiska unionens råd

Bryssel den 17 december 2025
(OR. en)

16960/25

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

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	11 december 2025
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	C(2025) 8407 final
Ärende:	KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/… av den 11.12.2025 om komplettering av Europaparlamentets och rådets förordning (EU) 2024/2847 genom att specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl till att skjuta upp spridningen av anmälningar

För delegationerna bifogas dokument – C(2025) 8407 final.

Bilaga: C(2025) 8407 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 11.12.2025
C(2025) 8407 final

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 11.12.2025

om komplettering av Europaparlamentets och rådets förordning (EU) 2024/2847 genom att specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl till att skjuta upp spridningen av anmälningar

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL DEN DELEGERADE AKTEN

Enligt Europaparlamentets och rådets förordning (EU) 2024/2847 (*cyberresiliensförordningen*) ska tillverkare av produkter med digitala element via en gemensam rapporteringsplattform anmäla alla aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för en produkt med digitala element. Enligt artikel 16.2 i den förordningen får den enhet för hantering av it-säkerhetsincidenter (*CSIRT-enhet*) som av medlemsstaten utsetts till samordnare och som först tog emot anmälan, under exceptionella omständigheter och på grundval av motiverade cybersäkerhetsrelaterade skäl, skjuta upp spridningen av anmälan till CSIRT-enheterna i de andra medlemsstater där produkten med digitala element har gjorts tillgänglig.

Denna delegerade akt är därför avsedd att komplettera cyberresiliensförordningen genom att specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl till att skjuta upp spridningen av anmälningar. Detta görs genom att identifiera tre typer av skäl till att den CSIRT-enhet som först tog emot anmälan får besluta att det är nödvändigt att skjuta upp ytterligare spridning till andra CSIRT-enheter. Ett sådant beslut om uppskjutande kan fattas i följande tre fall:

- Mot bakgrund av en bedömning av den anmälda informationens art.
- Om den CSIRT-enhet till vilken anmälan ska spridas inte kan säkerställa konfidentialiteten för sådan information.
- Om den gemensamma rapporteringsplattformen har kompromitterats eller tillfälligt inte är i drift.

De rapporteringsskyldigheter som anges i artikel 14 i förordning (EU) 2024/2847 ska tillämpas från och med den 11 september 2026.

2. SAMRÅD SOM FÖREGÅTT ANTAGANDET AV AKTEN

CSIRT-nätverket och Europeiska unionens cybersäkerhetsbyrå (Enisa) har rådfrågats om olika utkast till denna akt. En preliminär diskussion med vägledande frågor hölls den 26 mars 2025, med möjlighet att lämna skriftliga synpunkter fram till den 11 april 2025. Ett första utkast till denna akt delades med CSIRT-nätverket och Enisa den 16 maj 2025 och en diskussion hölls den 6 juni 2025, med möjlighet att lämna skriftliga synpunkter fram till den 27 juni 2025. Ett andra utkast till akten delades med CSIRT-nätverket och Enisa den 23 juli 2025, med möjlighet att lämna skriftliga synpunkter fram till den 1 september 2025. Ett tredje utkast till akten delades med CSIRT-nätverket och Enisa den 25 september 2025 och en diskussion hölls den 9 oktober 2025, med möjlighet att lämna skriftliga synpunkter fram till den 27 oktober 2025.

Utkastet till akt var föremål för ett offentligt samråd mellan den 16 oktober 2025 och den 13 november 2025. Totalt inkom 34 svar från 31 unika uppgiftslämnare (en uppgiftslämnare lämnade in synpunkter genom fyra olika inlagor). Av dessa inkom 29,41 % från näringslivsorganisationer, 26,47 % från företag, 17,65 % från EU-medborgare, 14,71 % från

myndigheter, 5,88 % från icke-statliga organisationer och 5,88 % från akademiska institutioner/forskningsinstitutioner[1].

Den 22 oktober diskuterades utkastet också med expertgruppen för cybersäkerhet för produkter med digitala element (E03967), vars medlemmar omfattar medlemsstaternas myndigheter, Enisa, enskilda experter med personliga mandat och organisationer i vid bemärkelse (t.ex. företag, sammanslutningar och icke-statliga organisationer).

3. DEN DELEGERADE AKTENS RÄTTSLIGA ASPEKTER

Befogenheten att anta delegerade akter ges i artikel 14.9 i cyberresiliensförordningen, enligt vilken kommissionen senast den 11 december 2025 ska specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl till att skjuta upp spridningen av anmälningar.

[1] Procentsatserna återspeglar inte det faktum att samma uppgiftslämnare lämnade synpunkter genom fyra olika inlagor.

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…

av den 11.12.2025

om komplettering av Europaparlamentets och rådets förordning (EU) 2024/2847 genom att specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl till att skjuta upp spridningen av anmälningar

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen)[2], särskilt artikel 14.9, och

av följande skäl:

(1) Den enhet för hantering av it-säkerhetsincidenter (*CSIRT-enhet*) som utsetts till samordnare och som först tog emot anmälan om en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för en produkt med digitala element (*den CSIRT-enhet som först tog emot anmälan*) får under exceptionella omständigheter, särskilt på begäran av tillverkaren och mot bakgrund av den anmälda informationens känslighet, och på grundval av motiverade cybersäkerhetsrelaterade skäl, besluta att under en tidsperiod som är absolut nödvändig skjuta upp spridningen av anmälan via den gemensamma rapporteringsplattformen till de CSIRT-enheter som utsetts till samordnare på det territorium där den tillverkare som lämnade in anmälan har angett att produkten med digitala element har tillhandahållits (*de berörda CSIRT-enheterna*). Det är därför nödvändigt att fastställa villkoren för att tillämpa sådana skäl. När sådana skäl är tillämpliga får den CSIRT-enhet som först tog emot anmälan skjuta upp spridningen till berörda CSIRT-enheter under en tidsperiod som är absolut nödvändig, men måste inte göra det. Enligt artikel 16.2 i förordning (EU) 2024/2847 ska en CSIRT-enhet som först tog emot anmälan, om den beslutar att åberopa sådana skäl, omedelbart informera Europeiska unionens cybersäkerhetsbyrå (Enisa) om beslutet om uppskjutande och ange varför den skjuter upp spridningen samt när den kommer att sprida anmälan ytterligare.

(2) I enlighet med artikel 16.2 andra stycket i förordning (EU) 2024/2847 ska villkoren för att tillämpa de cybersäkerhetsrelaterade skäl som anges i den här förordningen inte tillämpas på Enisas tillgång till den anmälda informationen. Enisas tillgång till den anmälda informationen får endast begränsas under särskilt exceptionella omständigheter, t.ex. om tillverkaren i sin anmälan anger att ett av de tre villkor som avses i artikel 16.2 tredje stycket a, b eller c i förordning (EU) 2024/2847 är uppfyllt, och då endast i samband med den anmälan om sårbarhet inom 72 timmar som avses i artikel 14.2 b i förordning (EU) 2024/2847. I sådana fall är den enda information som

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

samtidigt ska göras tillgänglig för Enisa information om att tillverkaren har gjort en anmälan, allmän information om produkten med digitala element, information om den allmänna karaktären av utnyttjandet och information om att säkerhetsrelaterade skäl angetts.

(3) Tillgång till den anmälda informationen gör det möjligt för CSIRT-enheterna att få en överblick över säkerhetsmiljön på sitt territorium och att införa riskreducerande åtgärder, och därigenom öka den övergripande cybersäkerhetsnivån i unionen. Ytterligare begränsningar av spridningen av anmälningar mot bakgrund av den anmälda informationens art bör därför endast vara möjliga i fall där de cybersäkerhetsrisker som följer av ytterligare spridning, mot bakgrund av den anmälda informationens känslighet, väger tyngre än säkerhetsfördelarna för unionen, och dessa risker inte kan minskas på lämpligt sätt genom att införa begränsningar av hanteringen och vidaredelningen av anmälan genom lämpliga protokoll som används inom CSIRT-nätverket, såsom Traffic Light Protocol (TLP) eller Permissible Actions Protocol (PAP). Detta kan till exempel vara fallet om en tillverkare har informerat den CSIRT-enhet som först tog emot anmälan om att den förväntar sig att inom kort tillhandahålla en riskreducerande åtgärd (t.ex. en programfix). Det kan också vara fallet när den CSIRT-enhet som först tog emot anmälan beslutar att endast dela delar av en anmälan och dessa delar ändå är tillräckliga för att de berörda CSIRT-enheterna ska kunna säkerställa att de kan införa lämpliga riskreducerande åtgärder. Dessutom, och för att uppmuntra samarbete om identifiering av och information om sårbarheter mellan tillverkare, CSIRT-enheter och säkerhetsforskare, kan detta också vara fallet när CSIRT-enheten fungerar som betrodd mellanhand för ett pågående förfarande för samordnad delgivning av information om sårbarheter i den mening som avses i artikel 12.1 i Europaparlamentets och rådets direktiv (EU) 2022/2555[3]. I enlighet med artikel 16.6 i förordning (EU) 2024/2847 ska CSIRT-enheten i sådana fall, när den beslutar att skjuta upp spridningen av en anmälan, skjuta upp den under en period som inte är längre än vad som är absolut nödvändigt och till dess att de berörda parterna inom samordnad delgivning av information om sårbarheter har gett sitt samtycke till utlämnande.

(4) Informationen i anmälan kommer att hjälpa CSIRT-enheterna att fullgöra sina uppgifter i samband med riskreducering och incidenthantering. I sällsynta fall kan dock sådan information vara tillräcklig för att göra det möjligt att ta fram en metod för utnyttjande utan ytterligare forskning, till och med för aktörer med begränsade färdigheter och resurser. Om fientliga aktörer fick tillgång till informationen skulle unionens cybersäkerhet påverkas kraftigt, med tanke på hur lätt det är att utnyttja den. Detta skulle till exempel kunna vara fallet om en sårbar version av en programvara endast marginellt skiljer sig från tidigare, icke-sårbara versioner. Om den CSIRT-enhet som först tog emot anmälan i sådana fall anser att de cybersäkerhetsrisker som följer av ytterligare spridning inte kan reduceras tillräckligt genom begränsningar av hantering och vidaredelning, kan den besluta att skjuta upp spridningen till dess att en effektiv riskreducerande åtgärd, såsom en säkerhetsuppdatering eller användarvägledning, finns tillgänglig.

(5) Om en berörd CSIRT-enhet inte kan skydda den anmälda informationen tillräckligt kan fientliga aktörer få tillgång till känslig information och utnyttja den på hela den

[3] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

inre marknaden. Om det finns allvarliga farhågor om en berörd CSIRT-enhets förmåga att säkerställa den anmälda informationens konfidentialitet får den CSIRT-enhet som först tog emot anmälan därför besluta att skjuta upp spridningen av anmälan till just den CSIRT-enheten tills farhågorna har stillats. Detta kan vara fallet i situationer där en berörd CSIRT-enhet har drabbats av en cybersäkerhetsincident som påverkar dess förmåga att bedriva sin verksamhet på ett säkert sätt, eller om det finns bevis för eller information om att betydande brister har upptäckts i CSIRT-enhetens kapacitet, såsom allvarliga resursbegränsningar som äventyrar dess förmåga att utföra sina funktioner eller beroende av föråldrad eller sårbar programvara.

(6) Om den gemensamma rapporteringsplattform som inrättats enligt artikel 16 i förordning (EU) 2024/2847 har komprometterats av en cybersäkerhetsincident bör den CSIRT-enhet som först tog emot anmälan, för att förhindra att fientliga aktörer får tillgång till känslig information, skjuta upp spridningen via den gemensamma rapporteringsplattformen tills plattformens förmåga att säkerställa den anmälda informationens konfidentialitet har återställts.

(7) I enlighet med artikel 16.2 första stycket i förordning (EU) 2024/2847 behöver den CSIRT-enhet som först tog emot anmälan inte sprida en anmälan till någon annan berörd CSIRT-enhet om tillverkaren anger att produkten med digitala element endast tillhandahålls på marknaden i den medlemsstat där den CSIRT-enhet som först tog emot anmälan är belägen.

(8) Kommissionen har samrått med och inhämtat synpunkter från berörda parter vid utarbetandet av utkastet till delegerad akt och har samrått med expertgruppen för cybersäkerhet för produkter med digitala element.

(9) I enlighet med artikel 14.9 i förordning (EU) 2024/2847 har kommissionen samarbetat nära med det CSIRT-nätverk som inrättats enligt artikel 15 i direktiv (EU) 2022/2555 och Enisa vid utarbetandet av utkastet till delegerad akt.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Innehåll

I denna förordning anges villkoren för att tillämpa de cybersäkerhetsrelaterade skäl som avses i artikel 16.2 i förordning (EU) 2024/2847 vilka gör det möjligt för den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan i enlighet med artiklarna 14.1, 14.3, 15.1 och 15.2 i den förordningen att skjuta upp spridningen av anmälan till de CSIRT-enheter som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

(1) *CSIRT-enhet som först tog emot anmälan*: den CSIRT-enhet som utsetts till samordnare och som först tog emot anmälan i enlighet med artiklarna 14.1, 14.3, 15.1 och 15.2 i förordning (EU) 2024/2847.

(2) *berörd CSIRT-enhet*: den CSIRT-enhet som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits.

Artikel 3

Villkor för att tillämpa cybersäkerhetsrelaterade skäl som härrör från den anmälda informationens art

Den CSIRT-enhet som först tog emot anmälan får besluta att under en tidsperiod som är begränsad till vad som är absolut nödvändigt skjuta upp spridningen av anmälningar eller delar av dem till berörda CSIRT-enheter i fall där de cybersäkerhetsrisker som spridningen medför, mot bakgrund av den anmälda informationens känslighet, väger tyngre än säkerhetsfördelarna och dessa risker inte kan reduceras genom begränsningar av hantering eller vidaredelning av anmälan genom lämpliga protokoll, såsom Traffic Light Protocol (TLP) eller Permissible Actions Protocol (PAP), och när minst ett av följande villkor är uppfyllt:

(a) Tillverkaren har informerat den CSIRT-enhet som först tog emot anmälan om att en effektiv riskreducerande åtgärd, såsom en säkerhetsuppdatering eller användarvägledning, förväntas bli tillgänglig inom 72 timmar. Om en effektiv riskreducerande åtgärd inte görs tillgänglig inom den tidsramen ska den CSIRT-enhet som först tog emot anmälan sprida anmälan till de berörda CSIRT-enheterna.

(b) Informationen i anmälan anses, mot bakgrund av den anmälda aktivt utnyttjade sårbarhetens art, vara tillräcklig för att ta fram en metod för utnyttjande, särskilt när sårbarheten lätt kan identifieras och utnyttjas av aktörer med begränsade färdigheter och resurser. När en effektiv riskreducerande åtgärd, såsom en säkerhetsuppdatering eller användarvägledning, väl finns tillgänglig ska den CSIRT-enhet som först tog emot anmälan sprida anmälan till de berörda CSIRT-enheterna.

(c) Den CSIRT-enhet som först tog emot anmälan kan med de berörda CSIRT-enheterna dela information som är tillräcklig för att säkerställa att de berörda CSIRT-enheterna kan införa lämpliga riskreducerande åtgärder. När en effektiv riskreducerande åtgärd, såsom en säkerhetsuppdatering eller användarvägledning, väl finns tillgänglig ska den CSIRT-enhet som först tog emot anmälan sprida den fullständiga anmälan till de berörda CSIRT-enheterna.

(d) Den CSIRT-enhet som först tog emot anmälan om den aktivt utnyttjade sårbarheten har uppmärksammats på den som en del av en samordnad delgivning av information om sårbarheter för vilken CSIRT-enheten fungerar som betrodd mellanhand i enlighet med artikel 12.1 i direktiv (EU) 2022/2555. I sådana fall ska den CSIRT-enhet som först tog emot anmälan, i enlighet med artikel 16.6 i förordning (EU) 2024/2847, sprida anmälan till de berörda CSIRT-enheterna när uppskjutandet inte längre är absolut nödvändigt och de parter som är involverade i den samordnade delgivningen av information om sårbarheter har gett sitt samtycke till utlämnande.

Artikel 4

Villkor för att tillämpa cybersäkerhetsrelaterade skäl med avseende på en specifik CSIRT-enhet

Den CSIRT-enhet som först tog emot anmälan får besluta att under en tidsperiod som är absolut nödvändig skjuta upp spridningen av anmälningar eller delar av dem till en specifik berörd CSIRT-enhet i fall där

(a) den berörda CSIRT-enheten har påverkats av en cybersäkerhetsincident som gör att dess förmåga att säkerställa den anmälda informationens konfidentialitet är ifrågasatt,

(b) den har tillräckliga skäl att tro att den berörda CSIRT-enheten inte har tillräcklig kapacitet för att säkerställa den anmälda informationens konfidentialitet.

I de fall som avses i första stycket a får den CSIRT-enhet som först tog emot anmälan skjuta upp spridningen tills den berörda CSIRT-enheten har informerat det CSIRT-nätverk som avses i artikel 15 i direktiv 2022/2555 om att dess förmåga att säkerställa konfidentialiteten för anmälan har återställts.

I de fall som avses i första stycket b får den CSIRT-enhet som först tog emot anmälan skjuta upp spridningen till den berörda CSIRT-enheten tills den CSIRT-enheten har lämnat bevis för att den har åtgärdat de identifierade bristerna.

Artikel 5

Villkor för att tillämpa cybersäkerhetsrelaterade skäl med avseende på den gemensamma rapporteringsplattformen

Den CSIRT-enhet som först tog emot anmälan får besluta att skjuta upp spridningen av anmälningar via den gemensamma rapporteringsplattform som inrättats genom artikel 16 i förordning (EU) 2024/2847 om Enisa i enlighet med artikel 16.4 i den förordningen har underrättat CSIRT-nätverket om att den gemensamma rapporteringsplattformen har påverkats av en cybersäkerhetsincident som väcker tvivel om dess förmåga att säkerställa den anmälda informationens konfidentialitet. I sådana fall får den CSIRT-enhet som först tog emot anmälan skjuta upp spridningen via den gemensamma rapporteringsplattformen tills Enisa har informerat CSIRT-nätverket om att plattformens förmåga att säkerställa anmälningarnas konfidentialitet har återställts.

Artikel 6

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 11.12.2025

På kommissionens vägnar
Ordförande
Ursula VON DER LEYEN