Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2026/881

20.4.2026

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2026/881

z dnia 11 grudnia 2025 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 poprzez określenie warunków zastosowania względów cyberbezpieczeństwa w odniesieniu do opóźniania rozpowszechniania zgłoszeń

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) ([1]), w szczególności jego art. 14 ust. 9,

a także mając na uwadze, co następuje:

(1) W wyjątkowych okolicznościach, a w szczególności na wniosek producenta i w świetle poziomu wrażliwości zgłoszonych informacji oraz z uzasadnionych względów cyberbezpieczeństwa, zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) wyznaczony jako koordynator, który jako pierwszy otrzymał zgłoszenie aktywnie wykorzystywanej podatności lub poważnego incydentu wywierającego wpływ na bezpieczeństwo produktu z elementami cyfrowymi („CSIRT, który jako pierwszy otrzymał zgłoszenie"), może podjąć decyzję o opóźnieniu – o okres absolutnie niezbędny – rozpowszechnienia zgłoszenia za pośrednictwem pojedynczej platformy sprawozdawczej do CSIRT-ów wyznaczonych jako koordynatorzy na terytorium, na którym, jak wskazał producent dokonujący zgłoszenia, produkt z elementami cyfrowymi został udostępniony („odpowiednie CSIRT-y"). W związku z tym konieczne jest określenie warunków zastosowania takich względów. W przypadku gdy takie względy mają zastosowanie, CSIRT, który jako pierwszy otrzymał zgłoszenie, może opóźnić jego rozpowszechnienie do odpowiednich CSIRT-ów o okres, który jest absolutnie niezbędny, ale nie ma takiego obowiązku. Zgodnie z art. 16 ust. 2 rozporządzenia (UE) 2024/2847, w przypadku gdy CSIRT, który jako pierwszy otrzymał zgłoszenie, postanowi powołać się na takie względy, powinien niezwłocznie poinformować Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) o swojej decyzji o opóźnieniu i jej powodach oraz o tym, kiedy zamierza dalej rozpowszechnić dane zgłoszenie.

(2) Zgodnie z art. 16 ust. 2 akapit drugi rozporządzenia (UE) 2024/2847 określone w niniejszym rozporządzeniu warunki zastosowania względów cyberbezpieczeństwa nie mają mieć zastosowania do dostępu ENISA do zgłoszonych informacji. Dostęp ENISA do zgłoszonych informacji może zostać ograniczony jedynie w szczególnie wyjątkowych okolicznościach: jeżeli producent wskaże w swoim zgłoszeniu, że spełniony jest jeden z trzech warunków, o których mowa w art. 16 ust. 2 akapit trzeci lit. a), b) lub c) rozporządzenia (UE) 2024/2847, przy czym dotyczy to wyłącznie zgłoszenia podatności, którego należy dokonać w ciągu 72 godzin, o którym to zgłoszeniu mowa w art. 14 ust. 2 lit. b) rozporządzenia (UE) 2024/2847. W takich przypadkach jedynymi informacjami, które należy jednocześnie udostępnić ENISA, są informacje o tym, że producent dokonał zgłoszenia; ogólne informacje na temat produktu z elementami cyfrowymi; informacje o ogólnym charakterze exploita; oraz informacje o tym, że powołano się na względy bezpieczeństwa.

(3) Dostęp do zgłoszonych informacji umożliwia CSIRT-om uzyskanie ogólnego obrazu środowiska bezpieczeństwa na ich terytorium oraz wprowadzenie środków ograniczających ryzyko, co podnosi ogólny poziom cyberbezpieczeństwa w Unii. W związku z tym dalsze ograniczenia w rozpowszechnianiu zgłoszeń w świetle charakteru zgłaszanych informacji powinny być możliwe wyłącznie w przypadkach, w których – ze względu na wrażliwość zgłaszanych informacji – ryzyko w cyberprzestrzeni wynikające z dalszego rozpowszechniania przewyższa korzyści dla Unii w zakresie bezpieczeństwa, a ryzyka tego nie można odpowiednio ograniczyć poprzez nałożenie ograniczeń dotyczących postępowania ze zgłoszeniem lub dalszego udostępniania zgłoszenia za pomocą odpowiednich protokołów stosowanych w sieci CSIRT, takich jak protokół *Traffic Light Protocol* (TLP) lub protokół *Permissible Actions Protocol* (PAP). Może tak być na przykład w przypadku, gdy producent poinformował CSIRT, który jako pierwszy otrzymał zgłoszenie, że wkrótce zamierza wprowadzić środek łagodzący (np. poprawkę). Może tak być również w przypadku, gdy CSIRT, który jako pierwszy otrzymał zgłoszenie, zdecyduje się udostępnić jedynie części zgłoszenia, a części te są jednak wystarczające, aby odpowiednie CSIRT-y mogły zapewnić wprowadzenie odpowiednich środków ograniczających ryzyko. Ponadto, aby zachęcić do współpracy w zakresie identyfikacji i ujawniania podatności między producentami, CSIRT i ekspertami w obszarze bezpieczeństwa, może to również

([1]) Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

mieć miejsce w przypadku, gdy CSIRT działa jako zaufany pośrednik w ramach trwającej procedury skoordynowanego ujawniania podatności, o której mowa w art. 12 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([2]). W takim przypadku, gdy CSIRT podejmie decyzję o opóźnieniu rozpowszechnienia zgłoszenia i zgodnie z art. 16 ust. 6 rozporządzenia (UE) 2024/2847, CSIRT ma opóźnić je o okres nie dłuższy niż jest to absolutnie niezbędne i do czasu wyrażenia zgody na ujawnienie przez strony zaangażowane w skoordynowane ujawnienie podatności.

(4) Informacje zawarte w zgłoszeniu pomogą CSIRT w wypełnianiu ich zadań w kontekście ograniczania ryzyka i postępowania w przypadku incydentów. W rzadkich przypadkach takie informacje mogą jednak wystarczyć do opracowania – bez dodatkowych badań – techniki umożliwiającej wykorzystanie istniejącej podatności, nawet przez podmioty o ograniczonych umiejętnościach i zasobach. Gdyby podmioty działające w złym zamiarze miały dostęp do tych informacji, miałoby to poważny wpływ na cyberbezpieczeństwo Unii, biorąc pod uwagę łatwość ich wykorzystywania. Może tak być na przykład w przypadku, gdy wersja oprogramowania podatna na zagrożenia różni się jedynie nieznacznie od poprzednich wersji, które nie były podatne na zagrożenia. W takich przypadkach, jeżeli CSIRT, który jako pierwszy otrzymał zgłoszenie, uważa, że ryzyka w cyberprzestrzeni wynikającego z dalszego rozpowszechniania zgłoszenia nie można odpowiednio ograniczyć poprzez nałożenie ograniczeń dotyczących postępowania ze zgłoszeniem i jego dalszego udostępniania, może podjąć decyzję o opóźnieniu rozpowszechnienia zgłoszenia do czasu udostępnienia skutecznego środka ograniczającego ryzyko, takiego jak aktualizacja zabezpieczeń lub wytyczne dla użytkowników.

(5) Jeżeli odpowiedni CSIRT nie jest w stanie właściwie chronić zgłoszonych informacji, podmioty działające w złej wierze mogą uzyskać dostęp do informacji szczególnie chronionych i umieścić exploity na całym jednolitym rynku. W związku z tym, jeżeli istnieją poważne obawy co do zdolności odpowiedniego CSIRT do zapewnienia poufności zgłaszanych informacji, CSIRT, który jako pierwszy otrzymał zgłoszenie, może podjąć decyzję o opóźnieniu rozpowszechnienia zgłoszenia wyłącznie do tego odpowiedniego CSIRT-u do czasu rozwiania takich obaw. Może to mieć miejsce w sytuacjach, w których odpowiedni CSIRT został dotknięty incydentem cyberbezpieczeństwa mającym wpływ na jego zdolność do bezpiecznego działania lub gdy istnieją dowody lub informacje, że wykryto istotne niedociągnięcia w zdolnościach CSIRT, takie jak poważne ograniczenia zasobów osłabiające jego zdolność do wykonywania jego funkcji lub poleganie na przestarzałym oprogramowaniu lub oprogramowaniu podatnym na zagrożenia.

(6) Aby zapobiec dostępowi podmiotów działających w złym zamiarze do informacji szczególnie chronionych, w przypadku gdy w wyniku incydentu cyberbezpieczeństwa doszło do naruszenia bezpieczeństwa pojedynczej platformy sprawozdawczej ustanowionej na podstawie art. 16 rozporządzenia (UE) 2024/2847, CSIRT, który jako pierwszy otrzymał zgłoszenie, powinien opóźnić rozpowszechnianie zgłoszonych informacji za pośrednictwem pojedynczej platformy sprawozdawczej do czasu przywrócenia zdolności platformy do zapewnienia poufności zgłoszonych informacji.

(7) Zgodnie z art. 16 ust. 2 akapit pierwszy rozporządzenia (UE) 2024/2847 CSIRT, który jako pierwszy otrzymał zgłoszenie, nie musi przekazywać zgłoszenia do żadnego innego odpowiedniego CSIRT-u, jeżeli producent wskaże, że produkt z elementami cyfrowymi jest udostępniany wyłącznie na rynku państwa członkowskiego CSIRT-u, który jako pierwszy otrzymał zgłoszenie.

(8) Przygotowując projekt aktu delegowanego, Komisja skonsultowała się z odpowiednimi zainteresowanymi stronami i zasięgnęła ich opinii oraz skonsultowała się z grupą ekspertów ds. cyberbezpieczeństwa produktów z elementami cyfrowymi.

(9) Zgodnie z art. 14 ust. 9 rozporządzenia (UE) 2024/2847 przy przygotowywaniu projektu aktu delegowanego Komisja ściśle współpracowała z siecią CSIRT ustanowioną na podstawie art. 15 dyrektywy (UE) 2022/2555 oraz z ENISA,

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu określa się warunki zastosowania względów cyberbezpieczeństwa, o których mowa w art. 16 ust. 2 rozporządzenia (UE) 2024/2847, które umożliwiają CSIRT-owi wyznaczonemu jako koordynator, który jako pierwszy otrzymał zgłoszenie zgodnie z art. 14 ust. 1 i 3 oraz art. 15 ust. 1 i 2 tego rozporządzenia, opóźnienie przekazania zgłoszenia do CSIRT-ów wyznaczonych jako koordynatorzy na terytorium, na którym, jak wskazał producent, produkt z elementami cyfrowymi został udostępniony.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „CSIRT, który jako pierwszy otrzymał zgłoszenie" oznacza CSIRT wyznaczony jako koordynator, który jako pierwszy otrzymał zgłoszenie zgodnie z art. 14 ust. 1 i 3 oraz art. 15 ust. 1 i 2 rozporządzenia (UE) 2024/2847;

2) „odpowiedni CSIRT" oznacza CSIRT wyznaczony jako koordynator na terytorium, na którym, jak wskazał producent, produkt z elementami cyfrowymi został udostępniony.

Artykuł 3

Warunki zastosowania względów cyberbezpieczeństwa wynikających z charakteru zgłaszanych informacji

CSIRT, który jako pierwszy otrzymał zgłoszenie, może podjąć decyzję o opóźnieniu, o okres ograniczony do tego, co jest absolutnie niezbędne, rozpowszechnienia zgłoszeń lub ich części do odpowiednich CSIRT-ów, w przypadkach gdy – w świetle wrażliwości zgłoszonych informacji – ryzyko w cyberprzestrzeni, jakie stwarza rozpowszechnianie, przewyższa korzyści w zakresie bezpieczeństwa, a ryzyka tego nie można ograniczyć poprzez nałożenie ograniczeń dotyczących postępowania ze zgłoszeniem lub dalszego udostępniania zgłoszenia za pomocą odpowiednich protokołów, takich jak protokół *Traffic Light Protocol* (TLP) lub protokół *Permissible Actions Protocol* (PAP), oraz gdy spełniony jest co najmniej jeden z następujących warunków:

a) producent poinformował CSIRT, który jako pierwszy otrzymał zgłoszenie, że w ciągu 72 godzin ma zostać udostępniony skuteczny środek ograniczający ryzyko, taki jak aktualizacja zabezpieczeń lub wytyczne dla użytkowników; jeżeli w tym terminie nie zostanie udostępniony skuteczny środek ograniczający ryzyko, CSIRT, który jako pierwszy otrzymał zgłoszenie, przekazuje je odpowiednim CSIRT-om;

b) informacje zawarte w zgłoszeniu uznaje się, w świetle charakteru zgłoszonej aktywnie wykorzystywanej podatności, za wystarczające do opracowania techniki umożliwiającej wykorzystanie podatności, w szczególności gdy podatność może być łatwo zidentyfikowana i wykorzystana przez podmioty o ograniczonych umiejętnościach i zasobach; po udostępnieniu skutecznego środka ograniczającego ryzyko, takiego jak aktualizacja zabezpieczeń lub wytyczne dla użytkowników, CSIRT, który jako pierwszy otrzymał zgłoszenie, przekazuje je odpowiednim CSIRT-om;

c) CSIRT, który jako pierwszy otrzymał zgłoszenie, jest w stanie udostępnić odpowiednim CSIRT-om wystarczające informacje w celu zapewnienia, aby odpowiednie CSIRT-y mogły wprowadzić odpowiednie środki ograniczające ryzyko; po udostępnieniu skutecznego środka ograniczającego ryzyko, takiego jak aktualizacja zabezpieczeń lub wytyczne dla użytkowników, CSIRT, który jako pierwszy otrzymał zgłoszenie, przekazuje pełne zgłoszenie odpowiednim CSIRT-om;

d) CSIRT, który jako pierwszy otrzymał zgłoszenie aktywnie wykorzystywanej podatności, został o niej powiadomiony w ramach skoordynowanego ujawniania podatności, w odniesieniu do którego dany CSIRT działa w charakterze zaufanego pośrednika zgodnie z art. 12 ust. 1 dyrektywy (UE) 2022/2555; w takim przypadku i zgodnie z art. 16 ust. 6 rozporządzenia (UE) 2024/2847 CSIRT, który jako pierwszy otrzymał zgłoszenie, przekazuje je odpowiednim CSIRT-om, jeżeli opóźnienie nie jest już absolutnie konieczne i strony zaangażowane w skoordynowane ujawnianie podatności wyraziły zgodę na ujawnienie.

Artykuł 4

Warunki zastosowania względów cyberbezpieczeństwa w odniesieniu do konkretnego CSIRT-u

CSIRT, który jako pierwszy otrzymał zgłoszenie, może podjąć decyzję o opóźnieniu o okres absolutnie niezbędny rozpowszechniania zgłoszeń lub ich części do konkretnego odpowiedniego CSIRT-u, w przypadku gdy:

a) odpowiedni CSIRT został dotknięty incydentem cyberbezpieczeństwa, co budzi wątpliwości co do jego zdolności do zapewnienia poufności zgłaszanych informacji;

b) ma wystarczające powody, by sądzić, że zdolności odpowiedniego CSIRT-u są niewystarczające do zapewnienia poufności zgłaszanych informacji.

W przypadkach, o których mowa w akapicie pierwszym lit. a), CSIRT, który jako pierwszy otrzymał zgłoszenie, może opóźnić jego rozpowszechnienie do czasu, gdy odpowiedni CSIRT poinformuje sieć CSIRT, o której mowa w art. 15 dyrektywy (UE) 2022/2555, że przywrócono jego zdolność do zapewnienia poufności zgłoszeń.

W przypadkach, o których mowa w akapicie pierwszym lit. b), CSIRT, który jako pierwszy otrzymał zgłoszenie, może opóźnić jego rozpowszechnienie do odpowiedniego CSIRT-u do czasu, gdy ten CSIRT przedstawi dowody na to, że usunął stwierdzone niedociągnięcia.

Artykuł 5

Warunki zastosowania względów cyberbezpieczeństwa w odniesieniu do pojedynczej platformy sprawozdawczej

CSIRT, który jako pierwszy otrzymał zgłoszenie, może podjąć decyzję o opóźnieniu rozpowszechniania zgłoszeń za pośrednictwem pojedynczej platformy sprawozdawczej ustanowionej na mocy art. 16 rozporządzenia (UE) 2024/2847, w przypadku gdy ENISA poinformowała sieć CSIRT, zgodnie z art. 16 ust. 4 tego rozporządzenia, że pojedyncza platforma sprawozdawcza została dotknięta incydentem cyberbezpieczeństwa, co budzi wątpliwości co do jej zdolności do zapewnienia poufności zgłaszanych informacji. W takich przypadkach CSIRT, który jako pierwszy otrzymał zgłoszenie, może opóźnić jego rozpowszechnienie za pośrednictwem pojedynczej platformy sprawozdawczej do czasu, gdy ENISA poinformuje sieć CSIRT, że przywrócono zdolność tej platformy do zapewnienia poufności zgłoszeń.

Artykuł 6

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 11 grudnia 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN