CRA SINGLE REPORTING PLATFORM

Factsheet over het centrale meldingsplatform dat is ingesteld bij de verordening cyberweerbaarheid

Melding van incidenten en actief uitgebuite kwetsbaarheden via het centrale meldingsplatform (SRP)

Wat?

Met ingang van 11 september 2026 moeten fabrikanten op grond van de verordening cyberweerbaarheid (Cyber Resilience Act, CRA) melding maken van actief uitgebuite kwetsbaarheden en ernstige incidenten die gevolgen hebben voor de beveiliging van in de EU verkochte producten met digitale elementen.

De verordening cyberweerbaarheid verplicht opensourcesoftwarestewards bovendien om dergelijke voorvallen te melden voor zover zij betrokken zijn bij de ontwikkeling van producten met digitale elementen.

Voor wie geldt dit?

Fabrikanten

opensourcesoftwarestewards

Welke nieuwe rapportageverplichtingen gelden er voor u?

Het bij de verordening cyberweerbaarheid (CRA) ingestelde meldingsplatform is een onlinetool voor fabrikanten en waarmee zij aan hun meldingsverplichtingen kunnen voldoen om actief uitgebuite kwetsbaarheden en ernstige incidenten te melden. Het meldingsplatform is bedoeld om de rapportageverplichtingen binnen de EU te vereenvoudigen en bestaat uit een elektronisch systeem dat het mogelijk maakt om met één enkele melding alle relevante autoriteiten te informeren. Het platform bevat de nodige beveiligingsmaatregelen om de vertrouwelijkheid te waarborgen.

Wanneer een melding wordt gedaan, wordt automatisch informatie verzonden naar uw nationale CSIRT, die de melding in eerste instantie ontvangt, naar de nationale CSIRT's van andere lidstaten waar het product met digitale elementen beschikbaar is, en naar het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa).

Hoe weet u aan welk nationaal CSIRT u melding moet doen?

In het algemeen wordt het nationale CSIRT waaraan u via het platform melding moet doen, bepaald door de lidstaat waar uw hoofdvestiging is gevestigd Artikel 14, lid 7, van de verordening cyberweerbaarheid (CRA) bevat gedetailleerde informatie aan de hand waarvan u kunt bepalen aan welk nationaal CSIRT u melding moet doen.

Welke voorvallen moet u melden?

- **Actief uitgebuite kwetsbaarheden:** kwetsbaarheden in producten met digitale elementen waarvan bekend is dat zij momenteel door een kwaadwillige actor worden uitgebuit, zoals bedoeld in artikel 3, punt 42, van de verordening cyberweerbaarheid.
- **Ernstige incidenten:** incidenten die ernstige gevolgen hebben voor de beveiliging van het product met digitale elementen (bijvoorbeeld doordat zij de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid in gevaar brengen), als gedefinieerd in artikel 3, punt 44 – in artikel 14, lid 5, is vastgelegd welke incidenten als ernstig worden beschouwd.

Wanneer moet u dergelijke voorvallen melden?

Het meldingsproces begint op het moment dat u, als fabrikant of opensourcesoftwaresteward, kennis krijgt van een actieve uitbuiting van een kwetsbaarheid of van een ernstig incident. Bij uw melding moet u de volgende termijnen in acht nemen:

Vroegtijdige waarschuwing

- binnen 24 uur nadat u kennis hebt gekregen van de kwetsbaarheid of het incident.

Melding van een actief uitgebuite kwetsbaarheid/een ernstige incident

- binnen 72 uur nadat u er kennis van hebt gekregen; in de melding moet algemene informatie worden verstrekt en een eerste beoordeling worden gemaakt.

Eindverslag:

- voor kwetsbaarheden: uiterlijk 14 dagen nadat een corrigerende maatregel (bijv. een patch) beschikbaar is gekomen.
- Voor ernstige incidenten: binnen 1 maand na de binnen 72 uur ingediende melding van het ernstige incident of de actief uitgebuite kwetsbaarheid.

CRA
SINGLE
REPORTING
PLATFORM

Wat gebeurt er nadat er een meldingen is ingediend?

Zodra er een meldingen is ingediend, zal het CSIRT dat de melding als eerste heeft ontvangen, de informatie onverwijld doorgeven aan de andere relevante CSIRT's in de EU-lidstaten waar het product ook verkrijgbaar is. De kennisgeving wordt tegelijkertijd doorgegeven aan Enisa.

De nationale CSIRT's delen bepaalde informatie ook met hun respectieve markttoezichtautoriteiten, opdat deze hun handhavingsverplichtingen kunnen nakomen.

Kan de verspreiding van informatie worden uitgesteld?

Ja, in uitzonderlijke gevallen kan de verspreiding van informatie worden uitgesteld overeenkomstig artikel 16, lid 2, van de verordening cyberweerbaarheid. In Gedelegeerde Verordening (EU) 2026/881 van de Commissie wordt nader gespecificeerd onder welke voorwaarden de verspreiding van meldingen kan worden uitgesteld.

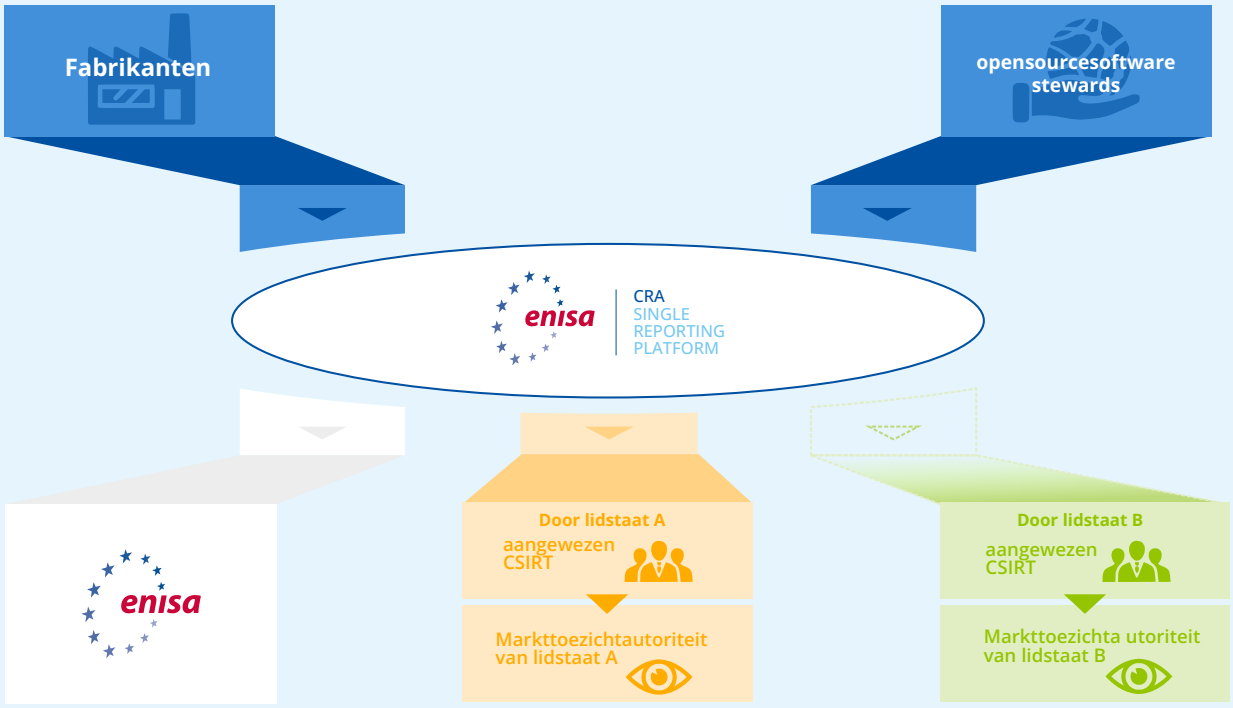
Hoe zou u het platform gebruiken?

1 Aanmelden

2 Nationale CSIRT selecteren

3 Gegevens invullen en versturen

Eenvoudige meldingsstroom



EUROPEAN UNION AGENCY FOR CYBERSECURITY

Voor meer informatie kunt u de pagina van Enisa met veelgestelde vragen over het centrale meldingsplatform raadplegen op https://www.enisa.europa.eu/cra-srp. Daar vindt u ook verwijzingen naar de richtsnoeren van de Europese Commissie inzake de verordening cyberweerbaarheid, die een nadere toelichting op de rapportageverplichtingen bevatten (zie paragraaf 9.1 van de richtsnoeren).

Voor ondersteuning kunt u contact opnemen met Enisa via : cra-srp.helpdesk@enisa.europa.eu.