enisa | CRA SINGLE REPORTING PLATFORM

Faktablad om den gemensamma rapporteringsplattformen för cyberresiliensförordningen

Rapportering av incidenter och aktivt utnyttjade sårbarheter via den gemensamma rapporteringsplattformen

Vad?

Från och med den 11 september 2026 ska tillverkare enligt cyberresiliensförordningen rapportera aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar säkerheten för produkter med digitala element som säljs på EU-marknaden.

Cyberresiliensförordningen kräver också att förvaltare av programvara med öppen källkod rapporterar dessa händelser i den mån de deltar i utvecklingen av produkter med digitala element.

För vem?

Tillverkare

Förvaltare av programvara med fri och öppen källkod

Vilka är mina nya rapporteringsskyldigheter?

Den gemensamma rapporteringsplattformen för cyberresiliensförordningen är ett onlineverktyg som tillverkare och förvaltare av programvara med öppen källkod kan använda för att uppfylla skyldigheten att rapportera aktivt utnyttjade sårbarheter och allvarliga incidenter. Den gemensamma plattformen är ett elektroniskt system som utformats för att göra det enklare att uppfylla EU:s rapporteringsskyldigheter, och som gör det möjligt att lämna in en enda rapport som når alla berörda myndigheter. Plattformen innehåller säkerhetsåtgärder för att skydda konfidentialiteten.

Genom varje anmälan kan du automatiskt skicka information till den nationella CSIRT-enheten som först mottar anmälan, till de andra nationella CSIRT-enheterna där produkten med digitala element är tillgänglig och till Europeiska unionens cybersäkerhetsbyrå (Enisa).

Hur vet jag vilken nationell CSIRT-enhet jag ska rapportera till?

I allmänhet är det i första hand ditt huvudsakliga verksamhetsställe som avgör till vilken nationell CSIRT-enhet du ska rapportera genom den gemensamma rapporteringsplattformen. Artikel 14.7 i cyberresiliensförordningen innehåller detaljerad information som hjälper dig att ta reda på vilken nationell CSIRT-enhet som du ska rapportera till.

Vilka händelser är jag skyldig att rapportera?

- **Aktivt utnyttjade sårbarheter:** Sårbarheter hos produkter med digitala element som man vet utnyttjas av en fientlig aktör, i enlighet med artikel 3.42 i cyberresiliensförordningen.
- **Allvarliga incidenter:** Incidenter som allvarligt påverkar säkerheten hos en produkt med digitala element (t.ex. genom att äventyra tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten) i enlighet med artikel 3.44; kriterierna för allvarlighetsgraden definieras i artikel 14.5.

När ska sådana händelser rapporteras?

Rapporteringsprocessen inleds när du, som tillverkare eller förvaltare av programvara med fri och öppen källkod, får kännedom om ett aktivt utnyttjande av en sårbarhet eller allvarlig incident. Följande tidsfrister ska iakttas:

Tidig varning

- Inom **24 timmar** efter att du har fått kännedom om sårbarheten eller incidenten.

Anmälan av aktivt utnyttjade sårbarheter/allvarliga incidenter:

- Inom **72 timmar** efter att du har fått kännedom. Anmälan ska innehålla allmän information och en första bedömning.

Slutrapport

- **För sårbarheter:** Senast 14 dagar efter att en korrigerande åtgärd har vidtagits (t.ex. en programfix).
- **För allvarliga incidenter:** Inom 1 månad efter anmälan av aktivt utnyttjad sårbarhet/allvarlig incident inom 72 timmar.

enisa | CRA SINGLE REPORTING PLATFORM

Vad händer när anmälningarna har lämnats in?

När anmälningarna har lämnats in ska den CSIRT-enhet som först tog emot anmälan utan dröjsmål sprida informationen till andra berörda CSIRT-enheter i de EU-medlemsstater där produkten också är tillgänglig. Anmälan görs samtidigt tillgänglig för Enisa.

De nationella CSIRT-enheterna kommer också att dela viss information med sina respektive marknadskontrollmyndigheter för att dessa ska kunna fullgöra sina tillsynsskyldigheter.

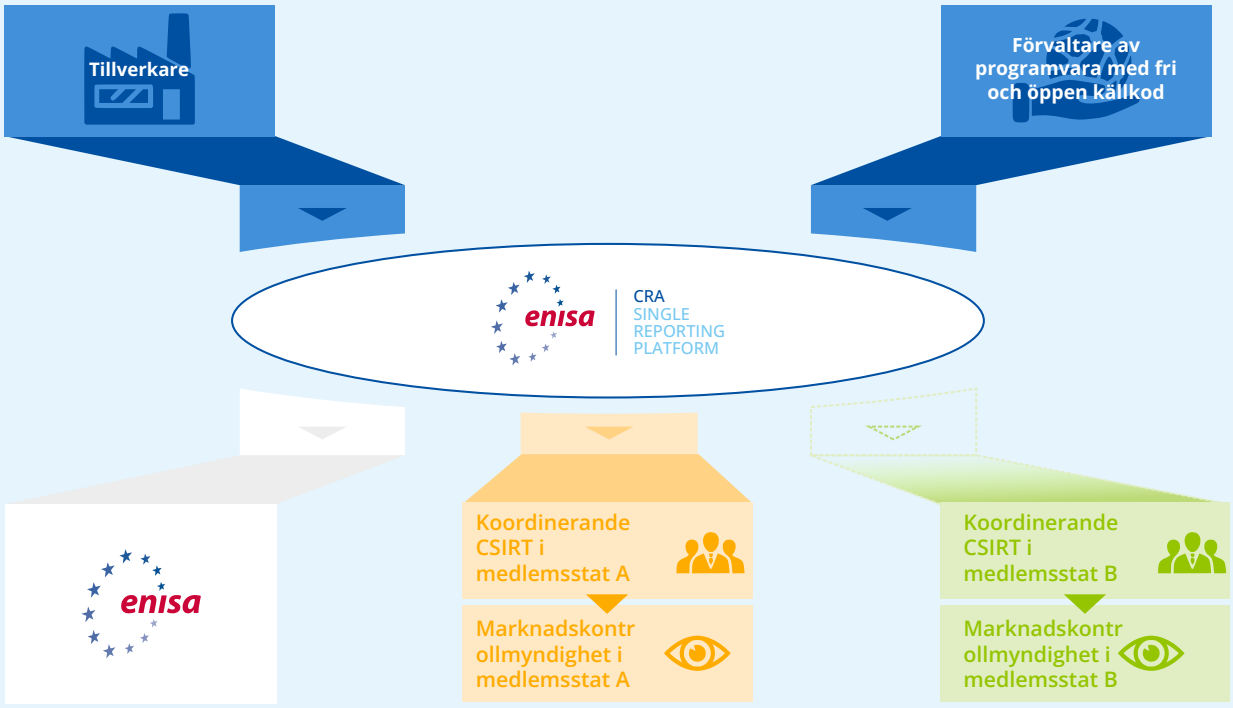
Kan spridningen av information skjutas upp?

Ja, under exceptionella omständigheter kan spridningen av information skjutas upp, i enlighet med artikel 16.2 i cyberresiliensförordningen. I kommissionens delegerade förordning (EU) 2026/881 anges närmare på vilka villkor spridningen av anmälningar får skjutas upp.

Hur ska jag använda plattformen?

1. Logga in
2. Välj nationell CSIRT-enhet
3. Ange information och lämna in

Enkelt rapporteringsflöde



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

För mer information, se sidan med vanliga frågor och svar om Enisas gemensamma rapporteringsplattform https://www.enisa.europa.eu/cra-srp, som även innehåller hänvisningar till Europeiska kommissionens vägledning om cyberresiliensförordningen, som i avsnitt 9.1 innehåller ytterligare förtydliganden om rapporteringsskyldigheter.

För support, kontakta: cra-srp.helpdesk@enisa.europa.eu.