

Fișă de informare privind Platforma unică de raportare pentru transmiterea notificărilor în temeiul Regulamentului privind reziliența cibernetică

Cum se raportează incidentele și vulnerabilitățile exploatare în mod activ prin platforma unică de raportare (SRP)?

■ Ce implică?

Începând cu 11 septembrie 2026, Regulamentul privind reziliența cibernetică obligă producătorii să raporteze vulnerabilitățile exploatare activ și incidentele grave care au un impact asupra securității produselor cu elemente digitale vândute pe piața UE.

Regulamentul privind reziliența cibernetică impune, de asemenea, administratorilor de software cu sursă deschisă să raporteze aceste evenimente, în măsura în care sunt implicați în dezvoltarea de produse cu elemente digitale.

■ Cui se adresează?



Producători



Administratori de software de tip open-source

■ Care sunt noile obligații de raportare care vă revin?

Platforma unică de raportare pentru transmiterea notificărilor în temeiul Regulamentului privind reziliența cibernetică este un instrument online care le permite producătorilor și responsabililor pentru software de tip open-source să-și îndeplinească obligația de a raporta vulnerabilitățile exploatare activ și incidentele grave. Concepută pentru a simplifica obligațiile de raportare la nivelul UE, platforma unică de raportare în temeiul Regulamentului privind reziliența cibernetică este un sistem electronic prin care raportați o

singură dată pentru a comunica tuturor autorităților relevante. Platforma include măsuri de securitate menite să protejeze confidențialitatea.

Fiecare notificare permite transmiterea automată a informațiilor către CSIRT-ul național care primește inițial notificarea, către celelalte CSIRT-uri naționale din statele în care produsul cu elemente digitale este disponibil și către Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

■ Cum aflați către ce CSIRT național trebuie să raportați?

În general, CSIRT-ul național către care trebuie să raportați prin intermediul platformei unice de raportare depinde în primul rând de locul unde aveți sediul. Articolul 14 alineatul (7) din Regulamentul privind reziliența cibernetică oferă informații detaliate care vă permit să identificați CSIRT-ul național către care trebuie să raportați.

■ Ce tipuri de evenimente aveți obligația să raportați?

- **Vulnerabilități exploatare activ:** Vulnerabilități în produse cu elemente digitale despre care se știe că sunt exploatare în prezent de un atacator, în conformitate cu articolul 3 alineatul (42) din CRA.
- **Incidente grave:** Incidente care au un impact grav asupra securității produsului cu elemente digitale (de exemplu, afectând disponibilitatea, autenticitatea, integritatea sau confidențialitatea), în conformitate cu articolul 3 alineatul (44); criteriile de stabilire a gravității sunt definite la articolul 14 alineatul (5).

■ Când trebuie să raportați astfel de evenimente?

Procesul de raportare începe în momentul în care dumneavoastră, în calitate de producător sau administrator de software de tip open-source, luați cunoștință de exploatarea activă a unei vulnerabilități sau de un incident grav. Se impune respectarea următoarei cronologii:

Alertă timpurie



- În termen de **24 de ore** de la momentul în care luați cunoștință de vulnerabilitate sau incident.

Notificare privind o vulnerabilitate exploatare activ/incidente grave



- În termen de **72 de ore** de la momentul în care luați cunoștință, furnizând informații generale și o evaluare inițială.

Raport final



- **Pentru vulnerabilități:** Nu mai târziu de 14 zile de la momentul la care este disponibilă o măsură corectivă (de exemplu, o actualizare de securitate).
- **Pentru incidente grave:** În termen de 1 lună de la trimiterea notificării privind vulnerabilitatea exploatare activ/incidentul grav, ce a fost efectuată în termen de 72 de ore.

■ Ce se întâmplă după ce au fost trimise notificările?

După trimiterea notificărilor, CSIRT-ul care primește inițial notificarea va transmite apoi fără întârziere informațiile către alte CSIRT-uri relevante din statele membre ale UE în care produsul este, de asemenea, disponibil. Notificarea este pusă simultan la dispoziția ENISA.

CSIRT-urile naționale vor transmite, de asemenea, anumite informații autorităților naționale de supraveghere a pieței, pentru a le permite acestora să-și îndeplinească atribuțiile de asigurare a respectării legislației.

■ Poate fi amânată diseminarea informațiilor?

Da, în circumstanțe excepționale, diseminarea informațiilor poate fi amânată, în conformitate cu articolul 16 alineatul (2) din CRA. Regulamentul delegat (UE) 2026/881 al Comisiei detaliază în continuare condițiile în care diseminarea notificărilor poate fi amânată.

■ Cum se utilizează platforma?



1 Conectare



2 Selectați CSIRT-ul național



3 Completați informațiile și transmiteți

■ Flux simplu de raportare

