CRA SINGLE REPORTING PLATFORM

Informativni list o enotni platformi za poročanje iz akta o kibernetski odpornosti

Kako poročati o incidentih in aktivno izrabljenih ranljivostih izdelkov prek enotne platforme za poročanje?

Kaj?

Od 11. septembra 2026 morajo proizvajalci v skladu z aktom o kibernetski odpornosti poročati o aktivno izrabljenih ranljivostih izdelkov in resnih incidentih, ki vplivajo na varnost izdelkov z digitalnimi elementi, ki se prodajajo na trgu EU.

Akt o kibernetski odpornosti od upravljavcev odprtokodne programske opreme zahteva tudi, da poročajo o teh dogodkih, če so vključeni v razvoj izdelkov z digitalnimi elementi.

Za koga?

Proizvajalci

Upravljavci odprtokodne programske opreme

Kakšne so vaše nove obveznosti glede poročanja?

Enotna platforma za poročanje (SRP) iz akta o kibernetski odpornosti je spletno orodje za proizvajalce in upravljavce odprtokodne programske opreme, ki jim omogoča izpolnjevanje obveznosti glede poročanja o aktivno izrabljenih ranljivostih izdelkov in resnih incidentih. Elektronski sistem CRA SRP, zasnovan za poenostavitev obveznosti poročanja v EU, omogoča, da se poročilo predloži le enkrat, s čimer se obvestijo vsi pristojni organi. Platforma vključuje varnostne ukrepe za varovanje zaupnosti.

Vsako obvestilo omogoča samodejno posredovanje informacij vaši nacionalni skupini CSIRT, ki prvotno prejme obvestilo, drugim nacionalnim skupinam CSIRT, v katerih je na voljo izdelek z digitalnimi elementi, in Agenciji EU za kibernetsko varnost (ENISA).

Kako ugotovite, kateri skupini CSIRT morate prijaviti incident?

Na splošno je nacionalna skupina CSIRT, ki ji morate poročati prek enotne platforme za poročanje, odvisna predvsem od glavnega sedeža vaše proizvodnje. Člen 14(7) akta o kibernetski odpornosti vsebuje podrobne informacije, na podlagi katerih lahko opredelite nacionalno skupino CSIRT, ki ji je treba poročati.

O katerih dogodkih morate poročati?

- **Aktivno izrabljene ranljivosti:** ranljivosti izdelkov z digitalnimi elementi, za katere je znano, da jih trenutno izrablja zlonamerni akter, v skladu s členom 3(42) akta o kibernetski odpornosti.
- **Resni incidenti:** incidenti, ki močno vplivajo na varnost izdelka z digitalnimi elementi (npr. ogrožanje razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti) v skladu s členom 3(44); merila resnosti so opredeljena v členu 14(5).

Kdaj morate poročati o takih dogodkih?

Postopek poročanja se začne v trenutku, ko se kot proizvajalec ali upravljavec odprtokodne programske opreme seznanite z aktivno uporabo ranljivosti ali resnim incidentom. Upoštevati je treba naslednje časovne okvire:

Zgodnje opozarjanje

- v roku **24 ur** od trenutka, ko se ugotovi obstoj ranljivosti ali incidenta.

Obvestilo o aktivno izrabljeni ranljivosti/resnem incidentu

- v roku **72 ur** od trenutka, ko je jasno, kaj se je zgodilo, se zagotovijo splošne informacije in opravi začetna ocena.

Končno poročilo

- **za ranljivosti:** najpozneje 14 dni po tem, ko je na voljo popravni ukrep (npr. varnostni popravek);
- **za resne incidente:** v **enem mesecu** po predložitvi 72-urnega obvestila o dejavno izrabljeni ranljivosti/resnem incidentu.

CRA SINGLE REPORTING PLATFORM

Kaj se zgodi, ko so obvestila posredovana?

Ko so uradna obvestila posredovana, skupina CSIRT, ki je prvotno prejela obvestilo, informacije nemudoma posreduje drugim zadevnim skupinam CSIRT v državah članicah EU, v katerih je izdelek na voljo. Obvestilo se hkrati posreduje agenciji ENISA.

Nacionalne skupine CSIRT bodo nekatere informacije posredovale tudi svojim pristojnim organom za nadzor trga, da bodo ti lahko izpolnili svoje obveznosti v zvezi z izvrševanjem predpisov.

Ali je mogoče odložiti posredovanje obvestila?

Da, v izjemnih okoliščinah se lahko posredovanje obvestila odloži v skladu s členom 16(2) akta o kibernetski odpornosti. Delegirana uredba Komisije (EU) 2026/881 podrobneje določa pogoje, pod katerimi se lahko posredovanje obvestil odloži.

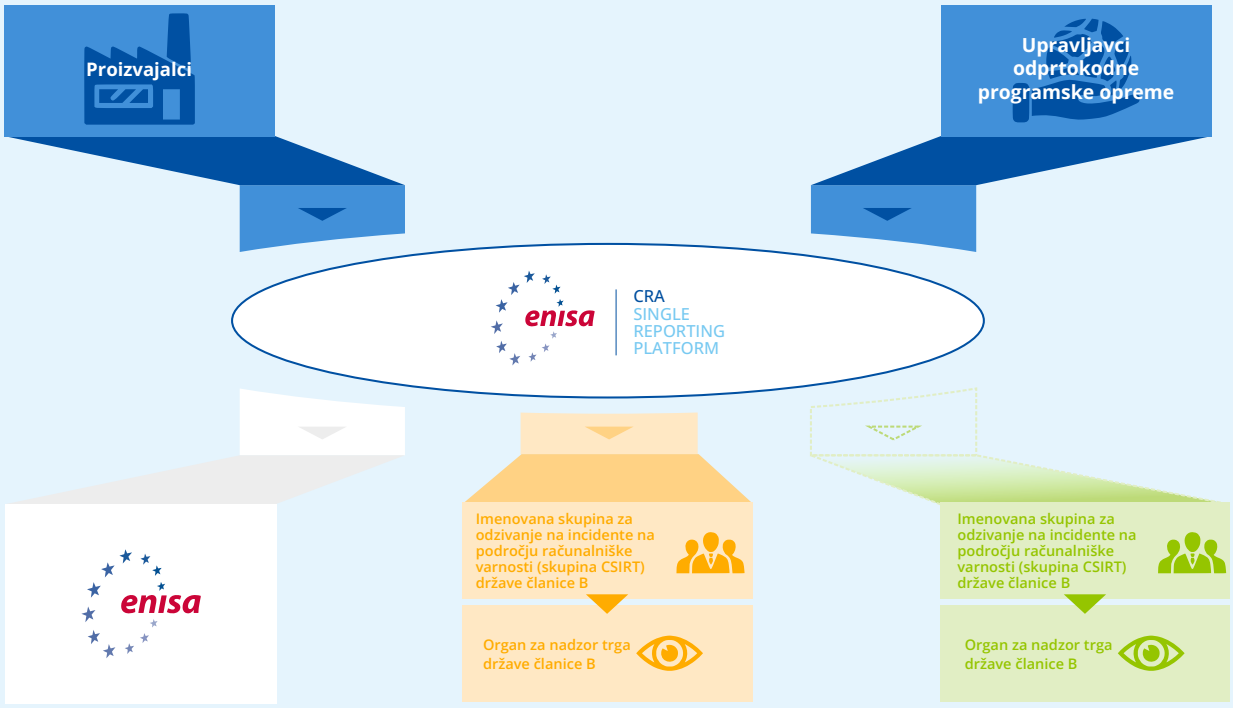
Kako se platforma uporablja?

1 Prijava

2 Izberite nacionalno skupino CSIRT

3 Izpolnite podatke in pošljite

Preprost tok poročanja



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Za dodatne informacije si oglejte stran z najpogostejšimi vprašanji o enotni platformi za poročanje agencije ENISA na naslovu https://www.enisa.europa.eu/cra-srp, na katerem so na voljo tudi sklici na Smernice Evropske komisije o aktu o kibernetski odpornosti, ki v poglavju 9.1 vsebujejo dodatna pojasnila o obveznostih poročanja.

Za podporo pišite na: cra-srp.helpdesk@enisa.europa.eu.