

# Informativní přehled o jednotné platformě pro podávání zpráv podle aktu o kybernetické odolnosti

Jak podávat zprávy o incidentech a aktivně zneužívaných zranitelnostech prostřednictvím jednotné platformy pro podávání zpráv (SRP)

## O co se jedná?

Od 11. září 2026 akt o kybernetické odolnosti (CRA) vyžaduje, aby výrobci podávali zprávy o aktivně zneužívaných zranitelnostech a závažných incidentech majících dopad na bezpečnost produktů s digitálními prvky prodáváných na trhu EU.

Akt o kybernetické odolnosti rovněž vyžaduje, aby správci softwaru s otevřeným zdrojovým kódem tyto události hlásili, pokud se podílejí na vývoji produktů obsahujících digitální prvky.

## Cílová skupina



Výrobci



Správci softwaru s  
otevřeným  
zdrojovým kódem

## Jaké jsou vaše nové povinnosti v oblasti podávání zpráv?

Jednotná platforma pro podávání zpráv podle aktu o kybernetické odolnosti je on-line nástroj určený výrobcům a správcům softwaru s otevřeným zdrojovým kódem, který jim umožňuje plnit povinnost podávat zprávy o aktivně zneužívaných zranitelnostech a závažných incidentech. Jednotná platforma pro podávání zpráv podle aktu o kybernetické odolnosti (CRA SRP) je elektronický systém, jehož cílem je zjednodušit povinnosti v oblasti podávání zpráv v rámci EU.

Umožňuje podat zprávu jen jednou, přičemž tato zpráva je následně rozeslána všem příslušným orgánům. Tato platforma zahrnuje bezpečnostní opatření na ochranu důvěrnosti.

Každé oznámení umožňuje automatické zasílání informací vašemu národnímu týmu pro reakce na počítačové bezpečnostní incidenty (CSIRT), který jej obdrží jako první, dalším národním týmům CSIRT, kde je produkt s digitálními prvky k dispozici, a Agentuře EU pro kybernetickou bezpečnost (ENISA).

## Jak zjistíte, kterému národnímu týmu CSIRT byste měli podat zprávu o incidentu?

Obecně platí, že národní tým CSIRT, jemuž byste měli podávat zprávy prostřednictvím jednotné platformy pro podávání zpráv, se stanovuje především podle místa vaší hlavní provozovny. Čl. 14 odst. 7 aktu o kybernetické odolnosti obsahuje podrobné informace, které vám umožní zjistit, kterému národnímu týmu CSIRT je třeba podat zprávu o incidentu.

## Jaké události jste povinni oznámit?

- **Aktivně zneužívané zranitelnosti:** zranitelnosti v produktech s digitálními prvky, o kterých se ví, že je škodlivý aktér zneužívá, v souladu s čl. 3 odst. 42 aktu o kybernetické odolnosti.
- **Závažné incidenty:** incidenty, které mají závažný dopad na bezpečnost produktu s digitálními prvky (např. ohrožení dostupnosti, autenticity, integrity nebo důvěrnosti) v souladu s čl. 3 odst. 44, přičemž kritéria závažnosti jsou definována v čl. 14 odst. 5.

## Kdy musíte tyto události oznámit?

Proces podávání zpráv začíná v okamžiku, kdy se vy, jako výrobce nebo správce softwaru s otevřeným zdrojovým kódem, dozvíte o aktivně zneužívané zranitelnosti nebo o závažném incidentu. Je třeba dodržovat tyto lhůty:

### Včasně varování



- Včasné varování: do **24 hodin** od okamžiku, kdy se o zranitelnosti nebo incidentu dozvíte.

### Oznámení aktivně zneužívané zranitelnosti / závažného incidentu



- Oznámení aktivně zneužívané zranitelnosti / závažného incidentu: do **72 hodin** od okamžiku, kdy se o zranitelnosti nebo incidentu dozvíte, s poskytnutím obecných informací a počátečního posouzení.

### Závěrečná zpráva



- V případě **zranitelnosti**: nejpozději do **14 dní** od okamžiku, kdy bude k dispozici nápravné opatření (např. oprava).
- V případě **závažných incidentů**: do **1 měsíce** od podání oznámení o aktivně zneužívané zranitelnosti nebo závažném incidentu ve lhůtě 72 hodin.

## ■ Co se stane po podání oznámení?

Jakmile jsou oznámení podána, tým CSIRT, který obdrží oznámení jako první, je poté neprodleně předá dalším příslušným týmům CSIRT v členských státech EU, kde je produkt rovněž k dispozici. Oznámení je souběžně předloženo agentuře ENISA.

Národní týmy CSIRT rovněž budou sdílet některé informace se svými příslušnými orgány dozoru nad trhem, aby jim umožnily plnit jejich povinnosti v oblasti prosazování předpisů.

## ■ Lze rozesílání oznámení odložit?

**Ano**, za výjimečných okolností může být rozesílání oznámení odloženo v souladu s čl. 16 odst. 2 aktu o kybernetické odolnosti. Podmínky, za kterých může být rozesílání oznámení odloženo, dále upřesňuje nařízení Komise v přenesené pravomoci (EU) 2026/881.

## ■ Jak platformu používat?



1 Přihlášení



2 Výběr národního týmu CSIRT



3 Vyplnění informací a podání

## ■ Jednoduchý postup podávání oznámení

