Responsible Disclosure Policy

Verze dokumentu: 2026-07-25
Kategorie: disclosure

Provozovatel: Kibios s.r.o., IČO 29814995, se sídlem Brněnská 305/32, 664 44 Ořechov.
Kontakt: info@kibios.com
Online verze: https://kibios.com/pravni/responsible-disclosure-policy

Responsible Disclosure Policy Verze: 1.0 Účinnost od: 4. 8. 2026 Společnost: Kibios s.r.o., Brněnská 305/32, 664 44 Ořechov, IČO 298 14 995

1. Účel a rozsah

Tato Responsible Disclosure Policy stanoví zásady odpovědného oznamování a zveřejňování bezpečnostních zranitelností souvisejících se službami, systémy a produkty společnosti Kibios s.r.o. Cílem je zajistit, aby zranitelnosti byly:

- nahlášeny bezpečným způsobem,
- včas opraveny,
- zveřejňovány tak, aby byla minimalizována rizika pro klienty a uživatele.

Policy se vztahuje na všechny zranitelnosti týkající se systémů a služeb Kibios, bez ohledu na to, kdo je objeví (interní tým, klient, externí výzkumník).

2. Principy odpovědného zveřejňování

Při odpovědném zveřejňování zranitelností se uplatňují zejména tyto principy:

- zranitelnost je nejdříve nahlášena Kibios, aby měl možnost ji opravit,
- detaily zranitelnosti nejsou veřejně publikovány před dokončením opravy nebo před dohodnutým termínem,
- zveřejněné informace neumožňují snadné zneužití zranitelnosti,
- chrání se osobní údaje a citlivá data, která mohly být zranitelností dotčena.

3. Hlášení zranitelností

Zranitelnost se hlásí v souladu s Vulnerability Disclosure Policy, zejména přes:

- určený bezpečnostní e-mail (např. security@kibios.com),
- ticket systém Kibios,
- formulář na webu/portálu, je-li k dispozici.

Hlášení by mělo obsahovat:

- popis zranitelnosti a její dopad,
- systém / URL / IP, kterého se týká,
- kroky k reprodukci, případně testovací účet či scénář,
- technické detaily (bez sdílení citlivých dat nad nezbytný rámec).

4. Proces řešení a zveřejnění ze strany Kibios

Po nahlášení zranitelnosti Kibios:

- provede analýzu a klasifikaci (kritičnost, CVSS skóre),
- připraví a nasadí opravu nebo mitigaci,
- informuje dotčené klienty (pokud se jich zranitelnost týká),
- po dokončení opravy může zveřejnit shrnutí zranitelnosti a nápravných opatření.

Zveřejňované shrnutí obvykle obsahuje:

- typ zranitelnosti,
- dotčený produkt/službu (bez detailů konkrétních klientských implementací),
- stručný popis dopadu,
- informace o tom, že byla vydána oprava a doporučení pro klienty,
- případně poděkování reportérovi, pokud si to přeje.

5. Veřejné zveřejnění ze strany reportéra

Pokud reportér (bezpečnostní výzkumník, klient, jiný subjekt) plánuje zveřejnit informace o zranitelnosti:

- měl by nejprve zranitelnost nahlásit Kibios a poskytnout přiměřený čas na opravu,
- měl by s Kibios koordinovat načasování a rozsah zveřejnění tak, aby neohrozil klienty a uživatele,
- ve zveřejnění by neměly být uvedeny konkrétní exploity či detaily, které umožní snadné zneužití, dokud si Kibios a klienti neaktualizují systémy.

Kibios podporuje odpovědné zveřejňování a může s reportérem spolupracovat na podobě veřejné zprávy (blogpost, odborný článek, prezentace).

6. Co je považováno za neoprávněné zveřejnění

Za neoprávněné zveřejnění se považuje zejména:

- publikování detailů zranitelnosti bez předchozího upozornění Kibios,
- zveřejnění exploitů, PoC kódů nebo detailních technických návodů před opravou,
- sdílení citlivých dat (např. osobní údaje, přístupové údaje, interní informace) získaných v rámci testu,
- zveřejnění informací způsobem, který může vést k trestné činnosti nebo škodě pro klienty či Kibios.

V takovém případě si Kibios vyhrazuje právo bránit se právními prostředky, včetně uplatnění nároků na náhradu škody.

7. Ochrana osobních údajů a citlivých dat

Při hlášení a zveřejňování zranitelností je nutné:

- minimalizovat nakládání s osobními údaji a citlivými informacemi,
- anonymizovat nebo redigovat údaje, které by mohly identifikovat konkrétní osoby nebo klienty,
- respektovat GDPR, DPA a další relevantní právní předpisy.

Pokud zranitelnost vedla k porušení zabezpečení osobních údajů, postupuje se také podle Incident Response Policy a GDPR (čl. 33, 34).

8. Vztah k dalším dokumentům

Responsible Disclosure Policy doplňuje a navazuje na:

- Vulnerability Disclosure Policy,
- Acceptable Use Policy (AUP),
- Rules of Engagement (RoE) pro penetrační testy,
- Incident Response Policy,
- smluvní dokumentaci (MSA, VOP, DPA).

V případě rozporu mají přednost konkrétní ujednání v MSA/VOP a RoE pro daný test/projekt.

9. Poděkování a případné uznání

Kibios si váží odpovědného hlášení zranitelností. Pokud reportér jedná v souladu s touto policy:

- může být veřejně poděkováno (např. uvedení jména/nicku v „Hall of Fame“ nebo v publikované zprávě),
- případná forma uznání je vždy předem konzultována s reportérem.

10. Závěrečná ustanovení

- Responsible Disclosure Policy může být aktualizována v návaznosti na změny technologií, služeb nebo právního rámce.
- Aktuální verze této policy může být zveřejněna na webu Kibios nebo v klientském portálu.
- Policy je vyhotovena v českém jazyce; v případě překladu je rozhodující české znění.