Vulnerability 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/vulnerability-disclosure-policy

Vulnerability 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 Vulnerability Disclosure Policy stanoví pravidla pro hlášení a řešení zranitelností týkajících se služeb, systémů a produktů společnosti Kibios s.r.o.

Cílem je umožnit bezpečnostním výzkumníkům, klientům a dalším osobám odpovědně oznamovat zranitelnosti a podpořit jejich včasné odstranění.

Policy se vztahuje na:

- systémy a služby provozované nebo spravované Kibios,
- webové aplikace, API, infrastrukturu a další komponenty v rozsahu služeb Kibios.

2. Kdo může hlásit zranitelnost

Zranitelnost může Kibios nahlásit zejména:

- externí bezpečnostní výzkumník,
- klient nebo jeho dodavatel,
- uživatel služeb Kibios,
- jiný subjekt, který na zranitelnost narazí v rámci legitimního používání služeb.

3. Zásady odpovědného hlášení

Osoba, která hlásí zranitelnost („reporter“), se zavazuje:

- nezneužívat zranitelnost k získání neoprávněného přístupu nebo škodlivé činnosti,
- neprovádět testy s dopadem na dostupnost služeb (např. DoS/DDoS),
- minimalizovat jakýkoli negativní dopad na systémy, data a uživatele,
- nešířit detaily zranitelnosti třetím osobám před dokončením opravy nebo domluveným zveřejněním.

4. Kanály pro hlášení zranitelností

Zranitelnost lze nahlásit prostřednictvím:

- určené e-mailové adresy (např. security@kibios.com),
- ticket systému Kibios,

- případně formuláře na webu Kibios, pokud je k dispozici.

Hlášení by mělo obsahovat zejména:

- popis zranitelnosti,
- dotčený systém / URL / IP,
- kroky k reprodukci,
- případné screenshoty nebo ukázkové požadavky/odpovědi (redigované, bez citlivých dat).

5. Postup Kibios po nahlášení zranitelnosti

Po přijetí hlášení Kibios:

- potvrdí přijetí hlášení reportérovi (pokud jsou k dispozici kontaktní údaje),
- provede základní ověření a klasifikaci (kritičnost, dopad, CVSS skóre),
- zahájí proces nápravy (oprava kódu, konfigurace, mitigace),
- informuje dotčené klienty, pokud se zranitelnost týká jejich systémů.

Kibios se snaží reagovat na hlášení v přiměřené lhůtě (např. do několika pracovních dnů) a kritické zranitelnosti řešit přednostně.

6. Zveřejnění informací o zranitelnosti

Po opravě zranitelnosti může Kibios:

- zveřejnit stručné technické shrnutí zranitelnosti a její nápravy (bez citlivých detailů),
- poděkovat reportérovi (pokud si to přeje a je to vhodné), např. uvedením jména nebo aliasu,
- využít poznatky pro zlepšení služeb, procesů a bezpečnostních opatření.

Veřejné zveřejnění plných technických detailů se může uskutečnit až po dokončení opravy a po zajištění, že uživatelé nejsou vystaveni zbytečnému riziku.

7. Co není povoleno při hledání zranitelností

Bez předchozího výslovného souhlasu Kibios není povoleno:

- provádět DoS/DDoS útoky nebo jiné testy narušující dostupnost,
- využívat nástroje nebo techniky, které mohou poškodit data nebo infrastrukturu,
- přistupovat k osobním údajům nad nezbytný rámec pro prokázání existence zranitelnosti,
- kopírovat, stahovat nebo zveřejňovat data získaná v důsledku zranitelnosti,
- provádět testy na systémech třetích stran, které Kibios pouze spravuje, bez souhlasu vlastníka těchto systémů.

8. Právní rámec a dobrá víra

Pokud se reportér drží této Vulnerability Disclosure Policy a jedná v dobré víře:

- Kibios nebude vůči reportérovi uplatňovat právní nároky za samotné oznámení zranitelnosti,
- Kibios bude považovat hlášení za součást odpovědného přístupu k bezpečnosti.

Toto neplatí v případě, že reportér zranitelnost zneužije k trestné činnosti, škodě nebo neoprávněnému zásahu do systémů či dat.

9. Vztah k Responsible Disclosure a dalším dokumentům

Tato Vulnerability Disclosure Policy je úzce provázána s:

- Responsible Disclosure Policy (obecná pravidla odpovědného zveřejňování),
- Acceptable Use Policy (AUP),
- Rules of Engagement (RoE) pro penetrační testy,
- Incident Response Policy.

V případě rozporu mají přednost smluvní dokumenty (MSA/VOP) a konkrétní dohody (RoE) uzavřené pro jednotlivé testy/projekty.

10. Závěrečná ustanovení

- Vulnerability 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.