TOPiN-HUB Kft.

Responsible Disclosure Policy

Biztonsági sebezhetőség-bejelentési keretpolitika külső kutatók részére

Cg. 13-09-223835 — 2161 Csomád, József Attila utca 1.

Hatályos: 2026. május 1. napjától
Verzió: v1.0

1. Bevezető

A TOPiN-HUB Kft. (a továbbiakban: „TOPiN”) értékeli a külső biztonsági kutatók, etikus hackerek és ügyfelek által jelzett biztonsági sebezhetőségeket. A jelen Responsible Disclosure Policy (RDP) célja, hogy egyértelmű, bizalomerősítő keretet adjon a sebezhetőségek felfedezésének, jelentésének és kezelésének — mind a bejelentő, mind a TOPiN számára.

A TOPiN nem üzemeltet jelenleg formális bug-bounty programot; a jelen RDP viszont világos elvekkel rendelkezik arról, hogy milyen cselekmény minősül jóhiszemű, jogszerű kutatásnak a TOPiN infrastruktúrája vonatkozásában, és hogyan jár el a TOPiN a bejelentés után.

2. Scope — mit vizsgálhatsz

A jelen RDP az alábbi rendszerekre vonatkozik:

- topin.hu fő weboldal és aldomain-jei (marketing-oldal, dokumentáció);
- portal.topin.hu és app.topin.hu (control plane / ügyfél-portál);
- status.topin.hu (státusz-oldal);
- api.topin.hu (publikus és autentikált API-végpontok);
- a TOPiN-Cloud termékek, AMELYEKHEZ A KUTATÓ RENDELKEZIK SAJÁT ELŐFIZETÉSSEL (azaz csak saját VM-eken tesztelhetsz);
- a TOPiN mobil- és desktop-kliens alkalmazásai, ha lesznek, a jövőben.

Ha nem vagy biztos benne, hogy egy adott komponens a scope-on belül van-e, jelezd a bejelentés előtt: security@topin.hu.

3. Out of scope — tilos területek

A következő tevékenységek NEM minősülnek jóhiszemű kutatásnak, és emiatt jogi következményekkel járhatnak:

- Más TOPiN-ügyfelek VM-jének vagy adatainak elérése, támadása (kivéve saját VM);
- Alvállalkozói rendszerek (pl. OVH hardver-infrastruktúra) közvetlen támadása;
- Erőforrás-kimerítéses (DoS/DDoS/brute-force) támadások;
- Social engineering és phishing a TOPiN munkavállalói ellen;
- Fizikai behatolás, hardver-manipuláció;
- Felhasználói fiókok kompromittálása (akár TOPiN-dolgozóé, akár ügyfélé);
- Magánvéleményű platformokba való bejelentkezés lopott jelszóval;
- Sebezhetőségek nyilvánosságra hozatala a TOPiN-nel történő előzetes koordináció nélkül;
- Szabadon elérhető személyes adatok aktív gyűjtése vagy értékesítése (még akkor is, ha a bejelentés indítja azt).

4. Biztonságos teszt-környezet kialakítása

Ha komolyabb kutatást tervezel a TOPiN-Cloud termékein, kérjük, hozz létre külön teszt-előfizetést kifejezetten erre a célra. Ezt jelezd előre a security@topin.hu címen, és a TOPiN rövid, nem-kötelező megerősítést küld.

Hasznos eljárásrend:

- Használj saját, a kutatási célra létrehozott ügyfélfiókot;
- A teszt-VM-eken csak saját, szintetikus (nem valós) adatokat használj;
- A teszt során rögzítsd pontosan a hálózati forrás-IP-det és a kutatási időkeretet;
- Ne használd a kutatás során más TOPiN-ügyfél adatait, még szimulációként sem.

5. Bejelentés módja

A sebezhetőség bejelentésének preferált csatornája:

- E-mail: security@topin.hu
- PGP-kulcs: elérhető a https://topin.hu/.well-known/security.txt címen (security.txt RFC 9116 szerint);
- Tárgysor ajánlott formátum: „[RDP] <rövid vulnerability-cím>”.

A bejelentés tartalmazza:

- A sebezhetőség technikai leírását;
- Az érintett URL-t / végpontot / komponenst;
- Reproducible steps — lépésről-lépésre reprodukálás leírása;
- Proof-of-concept (PoC), ha rendelkezésre áll — de NE tárold vagy osszd meg érzékeny ügyfél-adatot (kitakarva, redaktáltan közölhető);
- A sebezhetőség becsült súlyossága (CVSS v3.1 vektor, ha van);
- A bejelentő neve vagy pseudonímje, e-mail-elérhetősége (ezzel is felveszed a kapcsolatot, hogy tudjunk válaszolni).

6. TOPiN elkötelezettségei (safe harbor)

A jóhiszemű, a jelen RDP keretei között tevékenykedő kutatók vonatkozásában a TOPiN vállalja:

- A bejelentés beérkezésétől számított 3 munkanapon belül visszaigazolást küld;
- A sebezhetőség súlyosságának becslését 7 munkanapon belül közli;
- Nem kezdeményez jogi eljárást olyan cselekmény miatt, amely a jelen RDP kereteit betartotta;
- Nem osztja meg a bejelentő személyes adatát harmadik féllel a bejelentő előzetes engedélye nélkül;

- A javítás időbeli ütemezéséről rendszeresen (legalább 2 hetente) tájékoztat;
- A javítás után — a bejelentő engedélyével — hall-of-fame-jegyzetet tesz közzé a TOPiN weboldalán (neve vagy pseudonímje);
- Ha a bejelentő a scope-on kívül tevékenykedett, de jóhiszeműen és nem okozott kárt, a TOPiN a jogorvoslati lépések megtételét ésszerűen megfontolja.

7. Vulnerability-életciklus a TOPiN oldalán

A bejelentett sebezhetőség a TOPiN belső eljárásrendje szerint az alábbi szakaszokon halad át:

#	Szakasz	Cél-határidő	Tevékenység
1	Fogadás	T+3 nap	A bejelentés iktatása, visszaigazolás küldése, vizsgálat kijelölése
2	Triage	T+7 nap	Reproducibility ellenőrzése, CVSS-becslés, scope-besorolás
3	Javítás-tervezés	T+14 nap	Javítási terv, érintett komponensek azonosítása, patch-ütemezés
4	Javítás (Critical/High)	T+30 nap	Éles javítás kiadása, tesztelés, deployment
5	Javítás (Medium/Low)	T+90 nap	Éles javítás kiadása, tesztelés, deployment (következő sprint-be építve)
6	Koordinált disclosure	Patch kiadása után 0–30 nap	A bejelentővel egyeztetve nyilvános közzététel (advisory, CVE-kérelem ha releváns, hall-of-fame említés)

8. Koordinált nyilvánosságra hozatal (coordinated disclosure)

A TOPiN a koordinált disclosure elvét követi: a bejelentő és a TOPiN együtt állapítja meg, mikor és milyen formában kerül nyilvánosságra a sebezhetőség. Alapvető elv: a javítás élesítése után, hogy az ügyfelek ne legyenek kitéve utólagos kockázatnak.

Amennyiben a bejelentő 90 napon túl is várni kénytelen a TOPiN részéről, és a javítás ésszerű magyarázat nélkül halasztódik, a bejelentő — előzetes értesítéssel — megkezdheti az egyoldalú nyilvánosságra hozatal előkészítését. A TOPiN viszont vállalja, hogy ilyen helyzet elkerülésére tájékoztatási csatornát tart fenn minden nyitott bejelentésre.

9. Tilos a privát adatokkal való visszaélés

Ha a kutatás során véletlenül ügyfél-adatba vagy személyes adatba ütköztél:

- Ne tárold, ne másold le, ne oszd meg senkivel;

- A bejelentésben kizárólag annyi információval hivatkozz rá, amennyi a reprodukcióhoz feltétlenül szükséges (pl. az adatmező neve, nem az értéke);
- Amennyiben véletlen másolat keletkezett, a bejelentéssel egyidejűleg töröld, és igazold a törlést;
- A TOPiN a jelen elvek betartása mellett elzárkózik a jogi eljárás kezdeményezésétől.

10. Bejelentő kompenzációja

A TOPiN jelenleg nem üzemeltet pénzdíjas bug-bounty programot. Ugyanakkor:

- A legértékesebb bejelentések nyomán a bejelentő köszönet-levelet és hall-of-fame-említést kap;
- Kiemelkedő, kritikus sebezhetőség esetén a TOPiN mérlegelheti TOPiN-Cloud-kedvezmény (pl. egy év ingyenes Geo-VM-használat) biztosítását;
- A TOPiN-nél dolgozó csapat tekintse a bejelentést együttműködő partner-szándéknak, és a következő szakmai egyeztetéseken (közösségi blog-poszt, konferencia-részvétel) a bejelentőt aktívan támogassa.

11. Kapcsolat

- E-mail: security@topin.hu
- Security.txt: https://topin.hu/.well-known/security.txt
- PGP-kulcs: a security.txt fájl tartalmazza az aktuális hash-t és a nyilvános kulcsot;
- Kapcsolattartó személy: Zsolt Maróthy ügyvezető (zsolt.marothy@topin.hu).

12. Felülvizsgálat

A jelen RDP-t a TOPiN évente egyszer felülvizsgálja, a beérkezett bejelentések tanulságait beépíti, és szükség esetén bővíti a scope-ot vagy módosítja a safe-harbor-ígéreteket. A bejelentők visszajelzéseit a policy fejlesztése során figyelembe veszi.