BUILDIFY CDE

Hlášení bezpečnostních zranitelností

Vydává	Buildify Digital s.r.o.
IČO / sídlo	29541743 · Korunní 2569/108, Vinohrady, 101 00 Praha 10
Zápis	Městský soud v Praze, sp. zn. C 447453
Verze / účinnost	1.0 · účinné od 1. září 2026
Kontakt	kluch@buildify.cz

1. K čemu to je a kam hlásit

1.1 Buildify Digital s.r.o., IČO 29541743, se sídlem Korunní 2569/108, Vinohrady, 101 00 Praha 10 (dále „Poskytovatel"), provozuje službu Buildify CDE. Chceme se o slabých místech dozvědět dřív než útočník. Pokud jste na nějaké narazili, dejte nám vědět.

1.2 Hlaste na **kluch@buildify.cz**, do předmětu napište „Bezpečnostní hlášení". Píšeme česky i anglicky.

1.3 Aby se s hlášením dalo pracovat, uveďte:

- popis zranitelnosti a jaký má dopad
- přesnou adresu nebo koncový bod, kterého se týká
- kroky k reprodukci, ideálně krok za krokem
- čas testování a IP adresu, ze které jste testovali
- snímky obrazovky, záznam požadavků nebo krátký ukázkový kód, pokud je máte
- jak vás máme kontaktovat zpět

1.4 Nezveřejňujte hlášení dřív, než se domluvíme podle článku 6. Neposílejte nám cizí osobní údaje ani obsah cizích dokumentů — stačí popsat, k čemu jste se dostali.

2. Co je v rozsahu

2.1 Testovat můžete tyto části služby:

- webová aplikace cde.buildify.cz
- rozhraní a identity server api.buildify.cz
- marketingový web buildify.cz včetně poptávkového formuláře
- **veřejná ověřovací stránka výtisku** dokumentu
- **plugin systém**, včetně vydávání a platnosti tokenů

3. Co v rozsahu není

3.1 Mimo rozsah jsou:

- infrastruktura a služby našich sub-zpracovatelů, tedy Google Cloud, Stripe, Brevo, MailerSend, Microsoft a Google — hlaste přímo jim
- pluginy třetích stran a vlastní pluginy zákazníků
- sesterský produkt bpulse, i když sdílí identity server; zranitelnost samotného identity serveru v rozsahu je

- zjištění bez prokázaného dopadu, například chybějící bezpečnostní hlavička nebo doporučení z best practice bez funkčního scénáře zneužití
- nepotvrzené výstupy automatických skenerů, které jste sami neověřili
- sociální inženýrství, phishing a jakýkoli kontakt na naše zaměstnance, zákazníky nebo dodavatele
- fyzické útoky na kanceláře a zařízení
- DoS, DDoS, zátěžové a výkonnostní testy
- útoky vyžadující už kompromitované zařízení nebo účet oběti

4. Pravidla testování

4.1 Testujte **jen na vlastních testovacích účtech a vlastních projektech**. Registrace zdarma je k dispozici.

4.2 Nepřistupujte k datům jiných zákazníků a nestahujte je. Pokud potřebujete prokázat, že přístup je možný, stačí minimální důkaz — jeden identifikátor, jeden název souboru.

4.3 Pokud se k cizím datům dostanete náhodou, **okamžitě přestaňte**, kopie smažte a hned nám to nahlaste. Kolik dat jste viděli, napište upřímně.

4.4 Neměňte a nemažte cizí data, nezakládejte zadní vrátka, neinstalujte nic trvalého a nesnažte se udržet přístup.

4.5 Nedělejte DoS a zátěžové testy. Automatické skenery držte na rozumné rychlosti, ať neshodíte provoz ostatním.

4.6 Dodržujte právní předpisy a nezveřejňujte nic, co by ohrozilo naše zákazníky.

5. Co za to slibujeme

5.1 Když hlášení dorazí, **potvrdíme jeho přijetí do 3 pracovních dnů**.

5.2 **Do 10 pracovních dnů** vám sdělíme, jak jsme zjištění posoudili: jestli ho uznáváme, jakou mu dáváme závažnost a co s ním budeme dělat.

5.3 Až do uzavření případu vás budeme informovat **nejméně jednou za 14 dnů**, i kdyby zpráva zněla, že se pracuje.

5.4 Pokud jste dodržel pravidla v článcích 3 a 4 a jednal v dobré víře, Poskytovatel proti vám **nepodnikne právní kroky** a vaše jednání **nepovažuje za neoprávněný přístup** ke službě ani za porušení obchodních podmínek. Případné technické zablokování vašeho účtu zrušíme.

5.5 Tento příslib má hranice. Nekryje nároky třetích osob, tedy našich zákazníků, sub-zpracovatelů ani jiných uživatelů, a nemá vliv na postup orgánů činných v trestním řízení. Nezavazujeme se je nijak ovlivňovat, ale pokud jste postupoval podle těchto pravidel, potvrdíme jim, že jste testoval s naším svolením.

6. Zveřejnění

6.1 O zveřejnění se domluvíme. Standardně platí, že hlášení můžete zveřejnit **90 dní** od potvrzení přijetí, nebo dřív, pokud je zranitelnost odstraněná a shodneme se na tom.

6.2 Když opravu nestíháme, řekneme proč a navrhneme nový termín. Neshodneme-li se, budeme s vámi rovní: zdůvodníme to, ale nebudeme vám bránit.

6.3 **Peněžní odměny nevyplácíme.** Program odměn zatím neprovozujeme a nechceme slibovat něco, co nemáme.

6.4 Za nahlášení vám poděkujeme na webu, pokud s tím budete souhlasit. Uvedeme jméno nebo přezdívku podle vašeho přání. Bez souhlasu vás nikde nezmiňujeme.

7. security.txt

7.1 Tento soubor máme na https://buildify.cz/.well-known/security.txt podle RFC 9116:

```
Contact: mailto:kluch@buildify.cz
Expires: 2027-08-31T21:59:59.000Z
Preferred-Languages: cs, en
Canonical: https://buildify.cz/.well-known/security.txt
Policy: https://buildify.cz/bezpecnost/hlaseni-zranitelnosti
```

7.2 Hodnotu Expires je nutné každý rok posunout, jinak soubor přestane podle RFC 9116 platit.