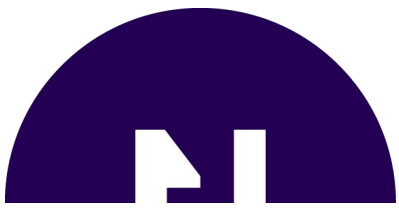
Možnosť plošného získania a zneužitia EÚ vakcinačných certifikátov

Ako na základe mena a dátumu narodenia získať EÚ vakcinačný preukaz ľubovoľného občana SR

Obsah



1 História zraniteľností

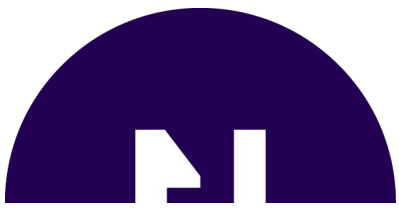
Podobne ako pri poslednej zraniteľnosti NCZI, kedy sme boli schopní stiahnuť všetky PCR/antigen testy a osobné informácie všetkých testovaných občanov, aj túto zraniteľnosť sme objavili čistou náhodou (čo znamená, **že sme nerealizovali žiadny cielený scan, nehľadali konkrétne zraniteľnosti, ale identifikovali sme ju pri bežnom používaní aplikácie**).

Cestoval som z Kyjeva do Bratislavy a pri vypĺňaní eHranica formulára som zadal iné kontaktné údaje (iný email, iné mobilné číslo) ako som zadal pri samotnej vakcinácii. Prekvapilo ma, že deň na to, som si nedokázal stiahnuť svoj EÚ COVID-19 certifikát a musel som kontaktovať NCZI supportné centrum. To mi síce nikdy neodpovedalo, ale prišiel som na to, že keď ako kontaktné údaje na získanie COVID-19-PASS zadám tie, ktoré som naposledy zadával pri vypĺňaní eHranica formulára, tak mi to COVID-19-PASS normálne prepošle a súčasne si dokážem stiahnuť svoj EÚ COVID-19 certifikát. Vtedy som si uvedomil, že týmto trikom dokážem získať COVID-19-PASS / EÚ vakcinačný preukaz prakticky akéhokoľvek človeka, ktorého rodné číslo poznám. Behom pár minút som našiel iný štátny web, ktorý mi dokázal pre konkrétne rodné číslo a meno overiť, či jeho rodné číslo je platné alebo nie. Jednoduchou enumeráciou som následne dokázal získať rodné číslo pre ľubovoľného človeka, ktorého dátum narodenia poznám. A potom som si všimol, že väčšina politikov a celebrít má svoj dátum narodenia uvedený na wikipédii a všetci ostatní na sociálnych sieťach...

Dátum nahlásenia zraniteľnosti CSIRT: 30.7.2021 o 18:23:43

Dátum potvrdeného prijatia zo strany CSIRT: 2.8.2021 o 8:32:35

Potvrdenie opravy uvedenej zraniteľnosti: 9.8.2021 o 11:59:24



2 Manažérske zhrnutie

Pred vyše mesiacom sme v článku “Prečo aj napriek GDPR prichádzame o súkromie a slobodu” nielenže kritizovali neschopnosť štátnych inštitúcií postarať sa o súkromie svojich občanov, ale predpovedali sme obrovské riziko úniku osobných údajov všetkých zaočkovaných občanov zo strany NCZI. Táto predpoveď sa bohužiaľ do mesiaca naplnila. **NCZI ani po tretí krát nebolo schopné ochrániť osobné dáta miliónov ľudí.**

Identifikovali sme spôsob, ako je možné získať EÚ vakcinačné preukazy všetkých zaočkovaných občanov - **na demonštráciu sme získali vakcinačné preukazy prominentných politikov**. A to iba na základe ich mena a dátumu narodenia dostupného na Wikipedii.

Toto sme dosiahli využitím viacerých kritických zraniteľností:

1. V aplikácii eHranica https://korona.gov.sk/ehranica/ sme identifikovali kritickú zraniteľnosť, pomocou ktorej sme dokázali získať kontrolu nad vakcinačným profilom ľubovoľného človeka. Na to, aby sme získali akékoľvek informácie o vakcinačnom profile daného človeka, nám stačí poznať len rodné číslo zaočkovaného.

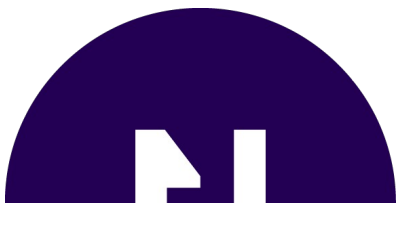
2. Využitím portálu https://www.portaludzs.sk/web/eportal/ sme zase našli spôsob ako enumeračným útokom získať rodné číslo akéhokoľvek človeka len na základe jeho mena a dátumu narodenia. Tento portál nám tiež umožnil overiť, ktoré z našich všetkých vygenerovaných mužských a ženských rodných čísel sú na Slovensku platné.

Vzhľadom k tomu, že do aplikácie eHranica dokáže ktokoľvek zaregistrovať kohokoľvek len na základe jeho mena a dátumu narodenia (rodné číslo dokáže triviálne získať), je možné databázu NCZI ľahko kontaminovať falošnými údajmi.

Takto kontaminovaná databáza nielenže nemá žiadnu výpovednú hodnotu, ale naopak môže viesť k nesprávnemu a nespravodlivému vynucovaniu pravidiel (vrátane obmedzeniu pohybu ako je povinná karanténa) voči všetkým, ktorí napríklad nikam necestovali.

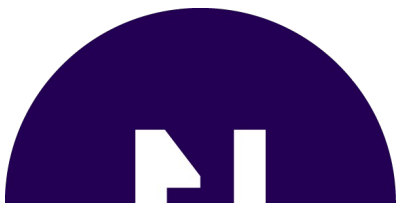
Vzhľadom na obrovský rozsah potenciálneho zneužitia (nehovoriac o tom, že aplikácia eHranica viedla k úniku všetkých EÚ vakcinačných preukazov), navrhujeme prevádzku aplikácie eHranica úplne ukončiť.

Podobne v situácii, kedy štátne inštitúcie ako NCZI nie sú OPAKOVANE schopné zabezpečiť ochranu osobných informácií miliónov občanov, sme



presvedčení, že je nevyhnutné zastaviť akékoľvek ďalšie plošné špehovanie občanov zo strany štátu (napríklad ukončiť prevádzku systémov na plošné špehovanie nakupovacieho správania občanov ako eKasa či eFaktura, kde hrozí ešte závažnejšie zneužitie).

Koncept rodného čísla vzhľadom na jeho veľmi obmedzenú množinu pokladáme za prekonaný a navrhujeme ho nepoužívať ako bezpečnostný identifikátor pre akékoľvek citlivé operácie (rodné číslo, ktoré sa používa ako heslo na šifrovanie vakcinačných certifikátov, sa nám podarilo prelomiť behom pár minút).



3 Ako na základe mena a dátumu narodenia získať EÚ vakcinačný preukaz ľubovoľného občana SR

3.1 Kritická zraniteľnosť v eHranica

Aplikácia https://korona.gov.sk/ehranica/ sa používa na registráciu všetkých občanov pri ceste zo zahraničia na Slovensko.

Pri návrate do krajiny musíte vyplniť dátum vášho návratu na Slovensko, z akej krajiny sa vraciate, vaše osobné údaje (meno, priezvisko, rodné číslo, prípadne ID pridelené inou krajinou, vašu emailovú adresu a mobilné číslo). Následne odškrtnete, či ste alebo nie ste vakcinovaní a teda súhlasíte s danou karanténou (alebo naopak ak ste vakcinovaní, tak do nej nejdete).

eHranica (podobne ako iné NCZI aplikácie) používa ako hlavný identifikátor rodné číslo a COVID-19-PASS identifikátor, ktorý je pre každého zaregistrovaného človeka unikátny.

Toto ale očividne neplatí pre **emailovú adresu a mobilné číslo, ktoré sú volatilné – aplikácia ich bez akýchkoľvek otázok mení a nastavuje na nové** (a zistili sme, že NCZI formuláre ich dokážu opakovane prepisovať).

Registráciu do NCZI systému ste vykonali napríklad pri úvodnom očkovaní, kde ste spolu so svojím rodným číslom zadali svoj email a mobilné číslo.

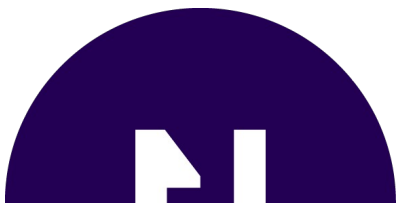
Napriek tomu, že NCZI od tohto okamihu pozná váš email a mobilné číslo, ktoré máte zviazané so svojím rodným číslom (a COVID-19-PASS), aplikácia eHranica od vás opätovne vyžaduje zadanie emailu a mobilného čísla (nestačí rodné číslo, ktoré s vašim emailom a mobilným telefónom už NCZI prepojené má).

Po vyplnení formulára aplikácia eHranica váš novo vyplnený email a mobilné číslo, ktoré ste tam uviedli spolu so svojím rodným číslom, automaticky nastaví ako nový kontaktný email a mobilné číslo vášho vakcinačného profilu (ktorý je jednoznačne identifikovaný vašim rodným číslom / COVID-19-PASS).

Toto zvláštne správanie totiž znamená:

Ak poznáte rodné číslo akéhokoľvek očkovaného človeka, tak mu vyplnením eHranica formuláru viete nastaviť nový kontaktný email a nové kontaktné mobilné číslo.

Po tejto zmene dokážete následne požiadať o vystavenie nového EÚ digitálneho certifikátu (https://covidforms.nczisk.sk/covid-19-validate-patient-gc.php), prípadne nového potvrdenia o očkovaní (https://vakcinacia.nczisk.sk/certifikat). Rovnako



môžete v mene “obete”, nad ktorou ste práve získali kontrolu robiť akékoľvek ďalšie operácie – napríklad registrovať sa na očkovanie, vykonávať zmeny v registrácii na očkovanie, upravovať osobné informácie, prípadne si vytvoriť nové prístupové údaje do GreenPass aplikácie.

Samozrejme, akékoľvek digitálne certifikáty, potvrdenia o očkovaní, autorizačné správy atď, sa posielajú už na nový email a nové mobilné číslo, ktoré ste pre dané rodné číslo nastavili pri vyplnení aplikácie eHranica.

Takže sa automaticky (okrem iného) dozviete, kedy sa daný človek očkoval, koľkými dávkami a akými presne vakcínami.

V praxi to znamená, že dokážete triviálne získať plnú kontrolu nad všetkými komunikačnými kanálmi akéhokoľvek človeka, ktorého rodné číslo poznáte a následne ich využiť na získanie alebo úpravu vašich citlivých informácií.

3.2 Ako na základe mena a dátumu narodenia získať rodné číslo kohokoľvek

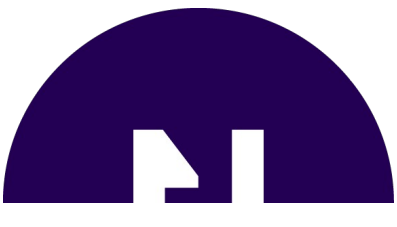
Netreba žiť v ilúzii, že rodné číslo predstavuje nejaký tajný osobný údaj. Ak vieme meno, priezvisko a dátum narodenia, tak ho dokážeme získať pre ľubovoľnú osobu relatívne dosť jednoducho (tých spôsobov je veľa, my sme sa rozhodli použiť len jeden z možných spôsobov).
Dátum narodenia je „defacto“ verejná informácia – pre politikov či celebrity ho viete získať z Wikipedie, pre všetkých ostatných ľudí napríklad zo sociálnych sietí (Facebook).

Keďže rodné číslo musí byť deliteľné číslom 11, pre každý dátum narodenia existuje maximálne 910 rodných čísel (10000 / 11 + 1). To je skutočne veľmi málo a prakticky vždy je ich možné odhaliť hrubou silou.

Vygenerovať všetky možné mužské a ženské rodné čísla je triviálne. Rodné číslo je možné vyjadriť v tvare RRMMDDXXXX a musí byť vždy deliteľné 11. Použili sme sadu triviálnych skriptov na vygenerovanie všetkých mužských a ženských rodných čísel (dohromady je ich 30 miliónov):

Skript na vygenerovanie mužských rodných čísel:

```
#!/bin/bash

for (( year=54; year < 100; year++));
do
  for (( month=1; month < 13; month++));
  do
    for (( day=1; day < 32; day++));
   do
```



```
        for (( suffix=0; suffix < 10000; suffix++));
    do
          final=$(( $year*100000000+$month*1000000+$day*10000+$suffix ));

          if (( final % 11 == 0 )); then
          printf "%010d\n" $final;
          fi
done
done
done
done
```

Skript na vygenerovanie ženských rodných čísel:

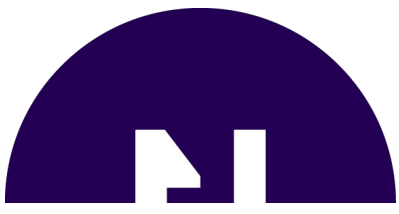
```
#!/bin/bash

for (( year=54; year < 100; year++));
do
  for (( month=1; month < 13; month++));
  do
    for (( day=1; day < 32; day++));
   do
        for (( suffix=0; suffix < 10000; suffix++));
    do
          final=$(( $year*100000000+($month+50)*1000000+$day*10000+$suffix ));

          if (( final % 11 == 0 )); then
          printf "%010d\n" $final;
          fi
   done
done
  done
done
```

Pred rokom 1954 sa používali 9.miestne rodné čísla, ktoré sa dajú vygenerovať ešte jednoduchším spôsobom.

Na overenie toho, ktoré z uvedených rodných čísel sú skutočne platné, sme použili verejne dostupnú službu “Overenie poistného vzťahu poistenca” https://www.portaludzs.sk/web/eportal/

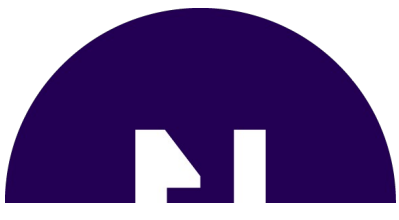
Uvedená služba síce používa CAPTCHu, ale jej cracknutie je triviálne a okrem toho sme prišli na to, že je chybne implementovaná a uvedený CAPTCHA kód je možné použiť opakovane (je na mieste podotknúť, že aj keby tá CAPTCHA bola implementovaná správne, tak využitím CAPTCHA resolving služieb je ju možné prakticky vždy prelomiť).

Behom pár minút dokážete cez hore uvedenú službu overiť validitu 910 vygenerovaných rodných čísel pre konkrétny dátum narodenia. Vypadnú vám rodné čísla desiatok ľudí, ktorí sa na Slovensku v daný dátum narodili. Po zadaní nepovinného údaju “Meno” a “Priezvisko” osoby, ktorú hľadáte, vám po jednoduchej iterácii vypadne rovno konkrétne jej rodné číslo.



Týmto spôsobom sme behom pár minút identifikovali rodné čísla viacerých prominentných politikov. Samozrejme, rovnako je možné identifikovať rodné číslo akéhokoľvek občana SR.

Keďže už máme rodné číslo hľadanej osoby, vraciame sa do sekcie 2.1 a cez zraniteľnosť v eHranica získavame plný prístup nad jej vakcinačným profilom (vrátane EÚ vakcinačného certifikátu).



4 Možnosť plošného získania a zneužitia EÚ vakcinačných certifikátov

Vyššie sme demonštrovali možnosť získania EÚ vakcinačného certifikátu alebo očkovacieho preukazu pre ľubovoľného človeka, ktoré meno a dátum narodenia poznáme.

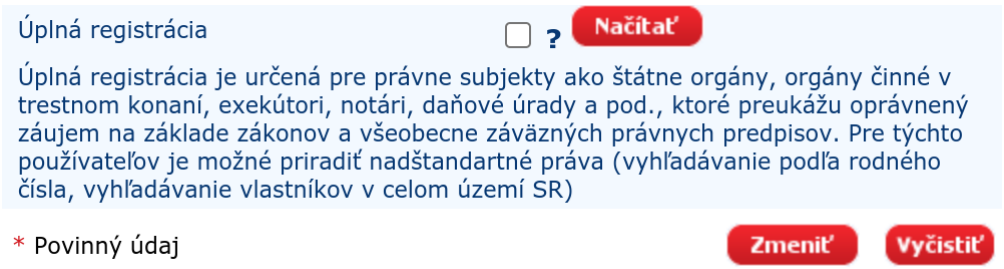
Existuje ale možnosť plošného získania vakcinačných certifikátov / očkovacích preukazov pre všetkých občanov EÚ. Stačí poznať ich rodné čísla a mená a následne aplikovať postup popísaný v kapitole 2.1.

Vyššie uvedené skripty vygenerujú 15 miliónov mužských a 15 miliónov ženských rodných čísel. Pomocou portálu https://www.portaludzs.sk/web/eportal/ je možné overiť, ktoré z nich sú platné a ktoré nie. A dostaneme zoznam 100% validných rodných čísel. Je potrebné podotknúť, že občania, ktorí na Slovensku nemajú trvalý pobyt, tak tam zrejme nemajú ani platné zdravotné poistenie.

Otázka znie, ako z tohto zoznamu platných rodných čísel získame mená ich vlastníkov. Našli sme viacero spôsobov ako je to možné (zrejme ich bude určite viac):

1. **Využitím katastra nehnuteľností**, kde každý list vlastníctva obsahuje meno, priezvisko a dátum narodenia vlastníka (a eviduje sa aj rodné číslo).

Právne subjekty ako štátne orgány, orgány činné v trestnom konaní, exekútori, notári, daňové úrady apod. môžu na katastri požiadať o tzv. “úplnú registráciu”, čo im umožní neobmedzené vyhľadávanie na základe rodného čísla, kedy dokážu jednoducho vyhľadať meno vlastníka nehnuteľnosti podľa jeho rodného čísla.



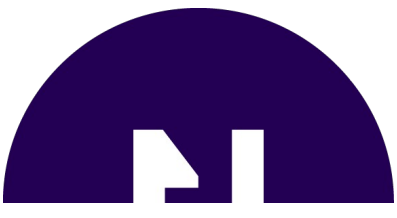
V kombinácii so zraniteľnosťou eHranica dokážu tieto subjekty získať EÚ vakcinačné certifikáty / očkovacie preukazy prakticky pre všetkých vlastníkov nehnuteľností na Slovensku.

2. **Využitím “leaknutého” katastra nehnuteľnosti**

Kataster nehnuteľností bol v minulosti veľakrát “vyharvestovaný” a informácie o všetkých vlastníkoch nehnuteľnosti unikli. Existujú teda uniknuté zoznamy veľkého množstva ľudí (vlastníkov nehnuteľností) a ich dátumov narodenia. Pre všetkých týchto ľudí je možné podľa sekcie 2.2 získať ich rodné čísla a následne podľa sekcie 2.1 získať ich EÚ vakcinačné certifikáty / očkovacie preukazy.

3. **Využitím Registra Obyvateľov (REGOB)**

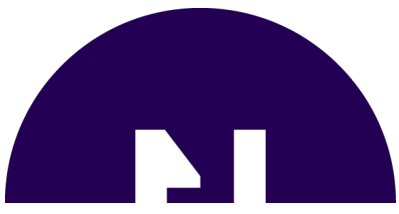
Do tohto registra má prístup veľké množstvo štátnych inštitúcií a iných právnych subjektov. Všetky tieto inštitúcie majú možnosť získať pre validné rodné čísla mená ich vlastníkov a následne podľa sekcie 2.1 získať ich EÚ vakcinačné certifikáty / očkovacie preukazy. A to plošne pre všetkých občanov SR.



5 Impersonifikačné útoky: Využívanie validného EÚ vakcinačného certifikátu svojho menovca

Plošné získanie väčšiny (alebo všetkých) EÚ vakcinačných certifikátov (popísané v sekcii 3) môže mať fatálne dôsledky. Popíšeme len jeden z nich. A to je napríklad možnosť impersonifikačných útokov. Nezaočkovaný človek môže získať plne digitálne validný EÚ vakcinačný certifikát svojho menovca (väčšina z nás má na Slovensku menovcov a je pravdepodobné, že pár z nich už bude zaočkovaných). Takto získaný 100% digitálne validný EU vakcinačný certifikát môže nezaočkovaná osoba využiť pri cestovaní, pri vstupe do reštaurácii a na všetky miesta, kde sú vyžadované očkovacie preukazy. Keďže nikto nepredpokladá, že niekto dokáže získať EÚ vakcinačný preukaz svojho menovca, prakticky nikto pri kontrole EU vakcinačného preukazu neoveruje dátum narodenia.

Je preto vysoko pravdepodobné, že možnosť impersonifikácie, kedy by ste ako nezaočkovaná osoba cestovala alebo inak využívala validný EÚ vakcinačný certifikát svojho menovca, by fungovala.



6 Možnosť kontaminovania NCZI databázy: Ako vrhnúť do karantény prakticky kohokoľvek

Demonštrovali sme, že cez aplikáciu eHranica je možné zaregistrovať svojho (ne)obľúbeného politika, prípadne akéhokoľvek človeka, ktorého meno a dátum narodenia poznáte (popis ako získať jeho rodné číslo je v sekcii 2.2). Ak za neho vyplníte „návrat“ z ľubovoľnej COVID-19 rizikovej krajiny a súčasne táto osoba nie je očkovaná (alebo neprekonala COVID-19), tak jej **automaticky hrozí povinná karanténa a znemožnenie voľného pohybu.** A to bez toho, aby sa táto osoba o tomto akokoľvek dozvedela (keďže pri jej registrácii síce použijete jej rodné číslo, ale použijete iný kontaktný email a mobilné číslo).

Celá aplikácia eHranica sa dá tým pádom triviálne kontaminovať a nedáva zmysel.

Keďže každý môže argumentovať, že ho do systému eHranica zaregistroval niekto iný, kto len vedel jeho dátum narodenia (napríklad z Facebooku, z ktorého následne získal rodné číslo), nie je možné v súčasnej dobe vynucovať akúkoľvek karanténu alebo iné pravidlá a to voči komukoľvek.

Vzhľadom na fakt, že eHranica sa dá ľahko kontaminovať falošnými údajmi, tak nielenže táto databáza nemá žiadnu výpovednú hodnotu, ale ešte naopak **môže viesť k nespravodlivému vynucovaniu pravidiel (ako karanténa) a to voči prakticky komukoľvek, koho meno a dátum narodenia poznáme.**

Vzhľadom na obrovský rozsah potenciálneho zneužitia (ako aj toho, že aplikácia eHranica viedla k úniku všetkých EÚ vakcinačných preukazov), navrhujeme prevádzku aplikácie eHranica úplne pozastaviť.

Sme totiž presvedčení o tom, že pravdepodobnosť zneužitia takto zbieraných informácií je vyššia ako pravdepodobnosť, že eHranica dokáže reálne pomôcť v efektívnom boji proti pandémii.