Possibility of widespread leak and misuse of EU vaccination certificates

How to get an EU vaccination card for any citizen of the Slovak Republic based on their name and date of birth

Table of Contents

1 Vulnerability history

Similar to our recent revealed vulnerability in the NCZI systems (NCZI or NHIC – National Health Information Center), where we were able to download 130 000 PCR/antigen tests and personal information of all tested citizens (90 000), we discovered this vulnerability by pure chance (meaning that **we did not perform any targeted scan, did not look for specific vulnerabilities, but identified it during normal use of the application**).

I was traveling from Kiev to Bratislava and when filling in the eHranica form I entered different contact details (different email, different mobile number) than I entered during the vaccination process itself. I was surprised that the day after, I could not download my EU COVID-19 certificate and had to contact NCZI support center. Although they never replied, I figured out that if I enter the contact details to get the COVID-19-PASS as the ones I entered last time when I filled out the eHranica form, it would normally send me the COVID-19-PASS and I would be able to download my EU COVID-19 certificate at the same time. That's when I realized that I can use this trick to get the COVID-19-PASS / EU vaccination certificate of virtually any person whose birth number I know. Within minutes, I found another government's website where I was able to verify for a specific birth number and name whether this birth number was valid or not. By simple enumeration, I was then able to get a birth number for any person whose birth date I know. And then I noticed that most politicians and celebrities have their date of birth listed on Wikipedia and everyone else on social media...

Vulnerability reporting date to CSIRT: 30.7.2021 at 18:23:43

Date of confirmed receipt by CSIRT: 2.8.2021 at 8:32:35

Confirmation of the fix for the vulnerability: 9.8.2021 at 11:59:24

2 Management summary

Over a month ago, in the article "Why we are losing privacy and freedom despite GDPR", we not only criticized the inability of state institutions to take care of the privacy of their citizens, but we predicted a huge risk of leakage of personal data of all vaccinated citizens by the NCZI (National Health Information Center). This prediction unfortunately came true within a month. For the third time, **the NCZI was unable to protect the personal data of millions of people.**

We have identified a way for the EU to obtain vaccination certificates of all vaccinated citizens - we **obtained vaccination certificates of prominent Slovak politicians for the demonstration**. This was possible only based on their name and date of birth available on Wikipedia.

We achieved this by exploiting several critical vulnerabilities:

1. We identified a critical vulnerability in eHranica https://korona.gov.sk/ehranica/ that we were able to use to gain control over the vaccination profile of any person. To obtain any information about a given person's vaccination profile, we only need to know the vaccinee's birth number.

2. Using the portal https://www.portaludzs.sk/web/eportal/, we again found a way to use an enumeration attack to obtain the birth number of any person based only on their name and date of birth. This portal also allowed us to verify which of our generated male and female birth numbers are valid in Slovakia.

Since anyone can register anyone in the eHranica application just on the basis of their name and date of birth (they can trivially obtain a birth number), the NCZI database can easily be contaminated with false data.

Such a contaminated database not only has no pandemic predictive value, but on the contrary can lead to incorrect and unfair enforcement of rules (including restrictions on movement such as mandatory quarantine) against anyone who has not traveled, as an example.

Given the huge scale of potential abuse (not to mention the fact that eHranica led to the leak of all EU vaccination certificates), we propose to shut down eHranica completely.

Similarly, in a situation where state institutions such as the NCZI are REPEATEDLY unable to ensure the protection of the personal information of millions of citizens, we believe that it is necessary to stop any further

massive spying on citizens by the state (for example, to stop the operation of systems for massive spying on citizens' shopping behavior such as eKasa or eFaktura, where there is a risk of even more serious abuse).

We consider the concept of the birth number obsolete due to its very limited set and suggest not to use it as a security identifier for any sensitive operations (we managed to crack the birth number, which is used as a password to encrypt vaccination certificates, in a few minutes).

3 How to get an EU vaccination card for any citizen of the Slovak Republic based on their name and date of birth

3.1 Critical vulnerability in eHranica

The https://korona.gov.sk/ehranica/ application is used to register all citizens traveling from abroad to Slovakia.

When returning to your country, you must fill in the date of your return to Slovakia, the country you are returning from, your personal data (first name, surname, birth number or ID number assigned by another country, your email address and mobile number). You then tick whether or not you are vaccinated and therefore agree to the quarantine (or if you are vaccinated, you do not go).

eHranica (like other NCZI applications) uses the birth number as the main identifier and the COVID-19-PASS identifier, which is unique for each registered person.

But this obviously doesn't apply to **email address and mobile number, which are volatile - the app changes and resets them without any questions** (and we've found that NCZI forms can overwrite them repeatedly).

For example, you registered in the NCZI system at the initial vaccination, where you entered your email and mobile number along with your birth number.

Although NCZI knows your email and mobile number from this point on, which are linked to your birth number (and COVID-19-PASS), the eHranica application requires you to enter your email and mobile number again (the birth number, which NCZI already has linked to your email and mobile phone, is not sufficient).

After you fill out the form, eHranica will automatically set your newly entered email and mobile number, along with your birth number, as the new contact email and mobile number for your vaccination profile (which is uniquely identified by your birth number / COVID-19-PASS).

This strange behavior means:

If you know the birth number of any vaccinated person, you can set up (and change) a new contact email and a new contact mobile number by filling in the eHranica form.

After this change, you can then apply for a new EU digital certificate (https://covidforms.nczisk.sk/covid-19-validate-patient-gc.php) or a new Slovak

vaccination certificate (https://vakcinacia.nczisk.sk/certifikat). You can also do any other operations on behalf of the "victim" you have just gained control over - for example, register for vaccinations, make changes to vaccination registration, edit personal information, or create new GreenPass app access credentials.

Of course, any vaccination certificates, authorization messages, etc., are already sent to the new email and mobile number that you set up for the birth number when you filled out the eHranica app.

You will therefore automatically know (among other things) when the person was vaccinated, how many doses, and exactly which vaccines.

In practice, this means that you can trivially gain full control over all the communication channels of any person whose birth number you know, and then use them to obtain or modify your sensitive information.

3.2 How to get the birth number of anyone based on their name and date of birth

There is no need to live under the illusion that the birth number represents some secret personal information. If we know the first name, last name and date of birth, we can get it for any person relatively easily (there are many ways, we decided to use only one of the possible ways).
The date of birth is "defacto" public information - for politicians or celebrities you can get it from Wikipedia, for all other people for example from social networks (Facebook).

Since the birth number must be divisible by 11, there is a maximum of 910 birth numbers for each birth date (10000 / 11 + 1). This is very few indeed, and can practically always be detected by brute force.

It is trivial to generate all possible male and female birth numbers. A birth number can be expressed in the form RRMMDDXXXX and must always be divisible by 11. We used a set of trivial scripts to generate all male and female birth numbers (there are 30 million in total):

Script to generate male birth numbers:

```
#!/bin/bash

for (( year=54; year < 100; year++)));
to
  for (( month=1; month < 13; month++)));
  to
    for (( day=1; day < 32; day++)));
   to
          for (( suffix=0; suffix < 10000; suffix++))
```

```
    to
        final=$(( $year*100000000+$month*1000000+$day*10000+$suffix ));

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

Script to generate female birth numbers:

```
#!/bin/bash

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

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

Before 1954, 9-digit birth numbers were used, which can be generated in an even simpler way.

To verify which of the above birth numbers are actually valid, we used the publicly available service "Verification of the insured person's insurance relationship". https://www.portaludzs.sk/web/eportal/

The above service did use CAPTCHA, but cracking it was trivial and besides, we found out that it is incorrectly implemented and the above CAPTCHA code can be reused (it is worth pointing out that even if the CAPTCHA was implemented correctly, it can practically always be broken by using more advanced CAPTCHA resolving services).

In a few minutes, you can use the above service to verify the validity of the 910 generated birth numbers for a specific date of birth. You will see the birth numbers of dozens of people who were born in Slovakia on that date. After entering the optional "First name" and "Last name" of the person you are looking for, after a simple iteration you will get their specific birth number.

In this way, we identified the birth numbers of several prominent Slovak politicians within minutes. Of course, it is also possible to identify the birth number of any citizen of the Slovak Republic.

Since we already have the birth number of the person we are looking for, we go back to section 2.1 and through a vulnerability in eHranica we get full access over their vaccination profile (including the EU vaccination certificate).

4 Possibility of widespread leak and misuse of EU vaccination certificates

Above we have demonstrated the possibility of obtaining an EU vaccination certificate for any person whose name and date of birth we know.

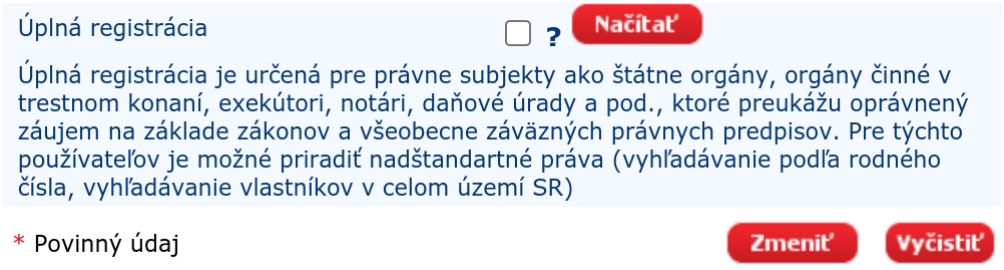
However, there is the possibility of massive leak of vaccination certificates for all Slovak citizens. It is sufficient to know their birth numbers and names and then apply the procedure described in chapter 2.1.

The above scripts will generate 15 million male and 15 million female birth numbers. Using the portal https://www.portaludzs.sk/web/eportal/ it is possible to check which of these are valid and which are not. And we get a list of 100% valid birth numbers. It should be noted that citizens who do not have permanent residence in Slovakia probably do not have valid health insurance there either.

The question is how do we get the names of the birth number owners from this list of valid birth numbers. We have found a number of ways to do this (there will probably be more):

1. **Using the Land Registry**, where each title deed contains the name, surname and date of birth of the owner (and the birth number is also recorded).

Legal entities such as state authorities, law enforcement agencies, bailiffs, notaries, tax authorities, etc. can apply for "full registration" at the cadastre, which will allow them to make unlimited searches on the basis of the birth number, where they can simply search for the name of the property owner by his birth number.



Combined with the vulnerability of eHranica, these entities are able to obtain EU vaccination certificates cards for virtually all property owners in Slovakia.

2. **Using the "leaked" land registry**
The cadastre of real estate has been harvested many times in the past and information about all property owners has been leaked. Thus, there are leaked lists

of a large number of people (property owners) and their dates of birth. For all these people it is possible to obtain their birth numbers under section 2.2 and then their EU vaccination certificates under section 2.1.

3. **Using the State Population Register (REGOB)**

A large number of state institutions and other legal entities have access to this register. All these institutions have the possibility to obtain the names of their owners for valid birth numbers and subsequently, according to section 2.1, to obtain their EU vaccination certificates. This is across the board for all citizens of the Slovak Republic.

5 Impersonation attacks: exploiting your namesake's valid EU vaccination certificate

The massive leak of most (or all) EU vaccination certificates (described in section 3) can have fatal consequences. We describe just one of them. Namely, the possibility of impersonation attacks. An unvaccinated person can obtain a fully digitally valid EU vaccination certificate for his or her namesake (most of us in Slovakia have namesakes, and it is likely that a few of them will already be vaccinated). The 100% digitally valid EU vaccination certificate thus obtained can be used by the unvaccinated person when traveling, when entering restaurants and all places where vaccination certificates are required. Since no one assumes that anyone can obtain their namesake's EU vaccination certificate, virtually no one verifies the date of birth when checking the EU vaccination certificate.

It is therefore highly likely that the option of impersonation, where you as an unvaccinated person would travel or otherwise use your namesake's valid EU vaccination certificate, would work.

6 Possibility of contamination of the NCZI database: How to quarantine virtually anyone

We have demonstrated that it is possible to register your (non-)favorite politician, or any person whose name and date of birth you know, through the eHranica application (see Section 2.2 for a description of how to get their birth number). If you fill in a "return" for him/her from any COVID-19 risk country and at the same time this person is not vaccinated (or has not passed COVID-19), he/she **is automatically at risk of mandatory quarantine and denial of free movement.** This is without the person having any knowledge of this (since you use their birth number when registering them, but you use a different contact email and mobile number and the given person is never notified).

The whole eHranica application can thus be trivially contaminated and makes no sense.

Since anyone can argue that they were registered in eHranica by someone else who only knew their date of birth (e.g. from Facebook, from which they subsequently obtained a birth number), it is currently impossible to enforce any quarantine or other rules on anyone.

Given the fact that eHranica can easily be contaminated with false data, not only does this database have no pandemic predictive value, but on the contrary, **it can lead to unfair enforcement of rules (like quarantine) against virtually anyone whose name and date of birth we know.**

Given the huge scale of the potential abuse (as well as the fact that eHranica led to the leak of all EU vaccination certificates), we propose to suspend eHranica completely.

In fact, we believe that the likelihood of misuse of the information massively collected in this way is higher than the likelihood that eHranica can realistically help in the effective fight against the pandemic.