

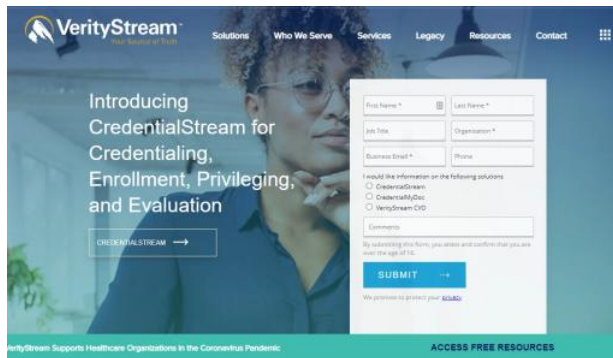
CVE-2021-32077 - FUN WITH SOCIAL SECURITY NUMBERS

06 May

06
May

In my day job I get a lot of time to spend with various software solutions which are meant to solve healthcare related problems with technology. It's fun, and it can be really surprising on how some software was designed and is continued to be used to accomplish daily tasks.

Today, I'll be writing about CVE-2021-32077. It's a vulnerability I discovered while reviewing the security configuration of a credentialing website. It's a really simple vulnerability and I don't think I'm breaking any new security research ground here. In healthcare, when employers of nurses, doctors, and other various healthcare workers need to have their credentials verified (ie, if they're licensed, what did they do, did they work for a hospital in the past, etc), they often turn to automated systems which can make this easy. One such piece of software is MSOW Solutions. This software is provided by VerityStream, or as they like to refer to themselves as 'your source of truth'.



The screenshot shows the VerityStream website with a navigation bar containing links for Solutions, Who We Serve, Services, Legacy, Resources, and Contact. The main content area features a large heading "Introducing CredentialStream for Credentialing, Enrollment, Privileging, and Evaluation" and a button labeled "CREDENTIALSTREAM". To the right is a registration form with fields for First Name, Last Name, Job Title, Organization, Business Email, and Phone. Below these fields are radio buttons for "CredentialStream", "Credentialing/Doc", and "VerityStream-CMS". A "SUBMIT" button is at the bottom of the form. At the very bottom of the page, there is a teal banner with the text "VerityStream Supports Healthcare Organizations In the Coronavirus Pandemic" and a link to "ACCESS FREE RESOURCES".

MSOW consists of a few components, the one which drew my initial attention was the PSV or Primary Source Verification search. This module had the ability to query users by PII information such as date of birth and social security serial number. This feature is meant to be used by anyone on the internet who is looking to verify the credentials of a provider.

MSOW VerityStream HarbaSec()

Primary Source Verification Search

We are pleased to provide this online primary source verification service to other hospitals, healthcare organizations and credentialing agents. It is not intended for use by patients or other visitors.

Thank you.

****Practitioner Last Name** and **Select facility** are required.**

Enter all or part of the physician's last name, complete and submit the form. Results will appear and can be printed as a credentialing verification letter.

Practitioner Last Name:

Birth date:

Last 4 digits of SSN: [Why?](#)

Last 4 digits of NPI:

Select facility:

Your Name:

Your Title:

Your Organization:

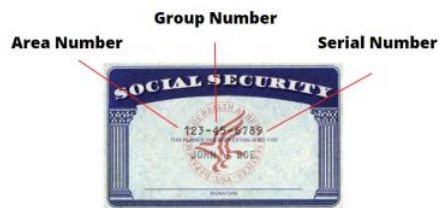
Verification Results

This internet facing component of MSOW's software inadvertently allows malicious users to query all employees in the company's database by their last name. Once obtained, a malicious user can target the discovery of the social security numbers by guessing possible numbers with automated fuzzing tools.

You might be saying to yourself: "Oh the last four of my social security number isn't really a big deal".

But it kinda is. The last four of your social security number, often known as the social security serial number - it's the one unique component in your social security number which isn't predetermined by how you began your life in the United States.

According to the Social Security Administration (SSA) (<https://www.ssa.gov/history/ssn/geocard.html>) in the United States, the nine digit number consists of three distinct values, the area number, group number and serial number.



The area number and the group numbers are assigned to groups of people who are in a specific geographical areas in specific times. Now, social security numbers are no longer issued this way, but had been up until June 25th, 2011 (<https://www.ssa.gov/employer/randomization.html>). While not failproof - typically armed with information such as a date of birth, name, and other details, researchers have been able to construct algorithms (<https://arstechnica.com/science/2009/07/social-insecurity-numbers-open-to-hacking/>) which guess the first 6 digits of a person's social security number with a high rate of success, something they used to verify with online credit card applications. Yikes.

The date of publishing this article is in 2021, meaning that every healthcare provider listed in these databases could likely have enough information siphoned off this way in order to commit fraud. (Unless of course if the provider is Doogie Howser and was born after 2011.)



There are of course, plenty of articles on data privacy and the horrors of having your social security serial number captured by a criminal - I won't link all those here, but in essence the last four can be used to apply for loans, utilize healthcare, perform various social engineering attacks, give you a bad day, and another reason to freeze your credit.

Thankfully, I'm writing this at the end of getting a coordinated disclosure for the vulnerability which the vendor patched (even though motivating them to do the right thing was as practical and easy as performing dental surgery on an elephant). I needed to get CERT (<https://kb.cert.org/involved>) and I used their brilliant VINCE system (<https://kb.cert.org/vince/>) (which I'll write about in a separate post) which helped make the vendor accountable for their software.

This was the final communication to customers which they mulled on sending to customers for almost two months after the patch was ready to go.

MarbaSec()

April 29, 2021

Client Notification

Dear MSOW Customer:

As always, the safety and security of your data is our priority. Your data has not been compromised, though we recently became aware of a vulnerability in connection with the MSOW Primary Source Verification (PSV) module. This vulnerability can be eliminated by applying a standard patch for MSOW v2.6.4 and above.


Please contact MSOW Support at [redacted] or email [redacted] and we will assist you with the patch installation. We recommend that you install this patch as soon as possible.

This patch mitigates the possibility that someone could guess the last four digits of an individual's Social Security number or birthdate combined with a last name when performing a primary source verification search on that individual. If the guess was successful, the provider's Social Security number or birthdate may be compromised. Once again, we have no reported instances where this has actually happened, but the patch removes the possibility.

Again, please contact us today to schedule a patch installation to eliminate this vulnerability. If, for some reason, you do not want to install the highly recommended patch, MSOW Support can walk you through another means to reduce the vulnerability.

We look forward to speaking with you and continuing to serve your needs.

Michael Sousa
President
VerityStream



Michael, it does feel a little disingenuous seeing that you had a fix for almost two months and you chose not to inform your customers as quickly as you could. So I'm a little disappointed here when you claim that 'the safety of your data is our priority'.

VerityStream reached out and patched their customers using MSOW on April 29th, 2021... hopefully closing the loop in a uncomplicated yet serious problem in a healthcare vendor's software.

Marbas

CVE-2021-32077 (/blog/tag/cve-2021-32077)

Healthcare (/blog/tag/healthcare)

Horrible Vendors (/blog/tag/horrible-vendors)

SSN (/blog/tag/ssn)

(https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.marbasec.com%2Fblog%2F2021-32077-fun-with-social-security-numbers&t=CVE-2021-32077+-+Fun+With+Social+Security+Numbers)

(https://twitter.com/intent/tweet?source=https%3A%2F%2Fwww.marbasec.com%2Fblog%2F2021-32077-fun-with-social-security-numbers&text=CVE-2021-32077+-+Fun+With+Social+Security+Numbers:%20https%3A%2F%2Fwww.marbasec.com%2Fblog%2F2021-32077-fun-with-social-security-numbers)

(https://pinterest.com/pin/create/button?url=https%3A%2F%2Fwww.marbasec.com%2Fblog%2F2021-32077-fun-with-social-security-numbers&description=CVE-2021-32077+-+Fun+With+Social+Security+Numbers)

(/rss.xml)

(/blog/cve-2021-22521-the-zen-of-privilege-escalation)

25

(/blog/cve-2021-22521-the-zen-of-privilege-escalation)

CVE-2021-22521 - The ZEN of Privilege Escalation (/blog/cve-2021-22521-the-zen-of-privilege-escalation)