Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

Author | Topic: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings (Read 2188 times)

warith (OP)
Newbie

Activity: 10
Merit: 51

WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 26, 2019, 11:49:55 PM #1

Merited by LoyceV (20), suchmoon (4), hugeblack (2), BitcoinGirl.Club (2), DdmrDdmr (2), vit05 (2), Pon13 (2), vapourminer (1), JayJuanGee (1), mocacinno (1), ABCbits (1), Tytanowy Janusz (1), AGD (1), eternalgloom (1)

-- Update 1 --
Please make sure to check my new reply to this post:
https://bitcointalk.org/index.php?topic=5114708.msg49967946#msg49967946

-- Update 2 -- [03/Mar/2019]

My second official statement regarding Coinomi wallet "Spell Check" scandal (video included):
https://twitter.com/warith2020/status/1102445902353043456

-- End of Update --

Please note that you can view a better version of this post here:
https://avoid-coinomi.com

TL;DR
Coinomi multi-asset wallet poor implementation leads to sharing your plain-text passphrase with a third-party server. My passphrase was compromised and $60K-$70K worth of crypto-currency were stolen because of Coinomi wallet and how the wallet handled my passphrase. I'm disclosing this issue publicly because Coinomi refused to take the responsibility and all my attempts through private channels have failed.

Please note that this security issue cannot be exploited by anyone except by the people who created it or have control over the backend. To everyone who is using or used Coinomi wallet, make sure to remove your funds from the wallet and change your passphrase by creating a new wallet using another application otherwise your funds might get stolen sooner or later.

To understand how catastrophic the security issue is, they simply take your crypto-currency wallet's passphrases/seeds and spell check it by sending it remotely to Google servers in clear plain text!

They did not take the responsibility of my loss, I gave them more than 24 hours before full disclosure, they fixed the issue without notifying their users and they kept procrastinating like scumbags to buy more time.

Below is a link to their final response to my request after going back and forth with them for over 3 days to get my stolen funds back, even after they confirmed the security issue and you can

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

clearly see how silly and reckless their responses are (these responses are just examples):
https://avoid-coinomi.com/files/coinomi_final_response.png

My advice never ever trust Coinomi with your hard earned crypto-currency assets. Read this post entirely to understand why because this is not their first time reflecting this kind behavior.

The Incident
First of all I admit it was my mistake trusting Coinomi wallet by inserting one of my main wallets (Exodus wallet) passphrase into their application. I trusted them because I downloaded the software from their website, the setup file was digitally signed and was mentioned by several reputable websites such as bitcoinwiki.org. I wanted to shift some of the assets that were not supported by Exodus wallet using the same passphrase/seed.

The incident began on 14th February, 2019. I downloaded and installed Coinomi application (Windows version) and noticed that their setup file was digitally signed but their main application was NOT signed after the installation process was completed.

I contacted them publicly through twitter (@warith2020) and they confirmed the issue then uploaded a new version with the main application signed. At that time I had already entered my Exodus's wallet passphrase into Coinomi's application.

On 22nd February 2019, I noticed that more than 90% of my Exodus wallet assets were transferred to multiple wallet addresses and the first transaction began with BTC on 19th February 2019 around 3:30 am UTC. Then followed by ETH (including ERC20 tokens), LTC and finally BCH.

Technical Analysis
I started going back in time and arranging the events. The only new thing that I did was installing and running Coinomi wallet so my first conclusion was that the unsigned version of the application had a backdoor.

I did further investigation and compared both the unsigned version of the setup file and the signed version. The only difference was they added digital signature to the main executable file and the Java file (the main application).

At that stage I thought that there is probably something suspicious about the application apart from having their main executable unsigned, so I started replicating what I did in a new virtual machine but this time I installed "Fiddler". A software that allows you to monitor and debug HTTP/HTTPS traffic of all applications running on your machine.

I started monitoring the traffic by running Fiddler in the background and then started Coinomi wallet. The first thing I noticed is that Coinomi application starts downloading dictionary wordlist from the following web address:
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-8-0.bdic

Then I clicked on restore wallet and pasted a random passphrase and suddenly the screen screamed SURPRISE MOTHER****** (boom puzzle solved!)

The WHOLE passphrase in plain-text is sent to googleapis.com a domain name owned by Google! It was sending it as a spelling check function! Here is sample of the screenshot of the HTTP request:
https://avoid-coinomi.com/files/coinomi_screenshot_1.png

To verify my findings I have uploaded a video for anyone who wants to test and replicate what I did:
https://avoid-coinomi.com/files/coinomi_http_traffic_video.mp4

You can also simply paste any random sentence with spelling mistake in the textbox in Coinomi's "Restore Wallet" form/page and you will see that it gets underlined with red line after being sent in clear text to googleapis.com.

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

To understand what's going on, I will explain it technically. Coinomi core functionality is built using Java programming language. The user interface is designed using HTML/JavaScript and rendered using integrated Chromium (Google's open-source project) based browser.

The whole thing is done using JxBrowser to build cross-platform applications and before you say (like Coinomi's CTO did) that it's JxBrowser issue, let me tell you that they mentioned this on their website in 2016 and how to disable the spell checking default behavior:
https://jxbrowser.support.teamdev.com/support/solutions/articles/9000044250-configuring-spell-checker

So essentially the textbox which you enter your passphrase in, is basically an HTML file ran by Chromium browser component and once you type or paste anything in that textbox it will immediately and discreetly send it remotely to googleapis.com for spelling check (how awesome is that!)

As a result, someone from Google's team or whoever had access to the HTTP requests that are sent to googleapis.com found the passphrase and used it to steal my $60K-$70K worth crypto assets (at current market price). Anyone who is involved in technology and crypto-currency knows that a 12 random English words separated by spaces will probably be a passphrase to a crypto-currency wallet!

Coinomi's Response
The team behind Coinomi are either extremely smart to add such backdoor so that when they get caught they would simply say it was an honest mistake or they are extremely stupid to overlook such security bug.

I will not be surprised if they intentionally created this backdoor behavior function and had an insider at Google especially when you learn from recent news about a founder of crypto-currency exchange claiming weird suspicious death while no one except him has access to the crypto-currency assets!

Coinomi's team did not reflect any responsible behavior and they kept asking me about the technical issue behind the bug because they were worried about their public image and reputation. They kept ignoring my request of taking the responsibility and ignored my solid facts regarding it. They didn't give a single **** about my stolen crypto assets. They kept reminding me (kinda threatening me) of the legal implications if I go public with the information I have and they forgot their legal responsibility for my stolen crypto assets as well as the risk that impacts other users of the wallet

In fact, Coinomi's team discreetly deleted their reply to my tweets to hide the evidence regarding their unsigned main executable in which they confirmed the issue and they didn't respond to my requests as shown in the following screenshots:
https://avoid-coinomi.com/files/coinomi_tweets.pdf

Such behavior was a clear evidence for me that there is something suspicious about their wallet and they didn't want to expose it. It seems the founders are the developers of the application and they don't like anyone who criticizes their ugly baby creation "Coinomi" wallet. They think that they are the code gurus fallen from the heavens who write perfect code.

However, before I published my findings I sent them the whole thing giving them more than 12 hours heads-up because they requested a clear technical evidence. Their CTO told me that he will download the report within 3 hours (they downloaded the report after 5-6 hours). Imagine someone tells you that you have a CRITICAL vulnerability in your software which holds users' hard earned crypto assets and yet you act carelessly because somehow you think you are a superior creature (Khan from Star Trek Into Darkness movie).

Below are the screenshots of the private messages between Coinomi's CTO and me:
https://avoid-coinomi.com/files/coinomi_cto_private_messages.pdf

This is not their first time behaving this way especially when someone finds an issue with their application. Luke Childs previously published a security vulnerability/misconfiguration and their

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

response was somehow similar:
https://bitsonline.com/coinomi-vulnerability-respond/
https://imnotdead.co.uk/blog/coinomi

Recap
To recap the events for further investigation:

- My first passphrase attempt was sent to googleapis.com through Coinomi wallet was on 14th February 2019
- Google's employee or whoever has control over the data that are sent to googleapis.com processed the data that had my passphrase and that was between 14th and 19th February 2019
- My crypto assets were stolen on 19th February 2019 starting around 3:30 am UTC and the transactions continued for 15 minutes. At the end 90% of the assets were gone and remaining assets were only left because these assets were supported by Exodus wallet but NOT Coinomi wallet (what a coincidence you say!)

Please note that I took all the security precaution to keep my passphrase and wallet safe. I have a separate isolated virtual machine for it with Anti-Virus/Anti-Malware and firewall installed. I also had other wallets on the same virtual machine for years. Nothing was stolen except for the wallet which I recently used my passphrase in, which is Coinomi wallet!

What's Next
I will start taking legal actions against the company behind Coinomi if they don't act and take the responsibility. The company is registered in UK as "Coinomi LTD" if anyone one has faced or facing similar case were you suddenly lost your crypto assets and you happen to have used Coinomi wallet. The funny thing is that they state on their website:
"Most importantly, no Coinomi wallet has ever been hacked or otherwise compromised to date."
(bull****!)

Be aware that probably all desktop versions are affected (I'm not sure about the mobile versions) and the guy/group who is/are capturing the passphrases, possibly targeting only wallets with decent amount of assets to stay low profile as long as he/they can.

I have also uploaded copy of the latest version of Coinomi application in case they take down the links to hide the facts:

- Download UNSIGNED version (proof that the main application was not signed)
- Download signed version (proof that the wallet sends passphrase to a remote server)
- Screenshot of the SHA256SUM hashes before the patch

Final Thoughts
This was an expensive and mentally painful experience to learn from and hopefully after publishing this post no one will experience the same. The lessons learned so far:

- Never trust any multi-asset crypto wallet unless they have done an external security audit by a trusted third-party and their security audit is publicly available.
- Never ever trust Coinomi with your hard earned crypto-currencies. They do not take any responsibility and when they f***-up things they just run away like it's not their business.
- Never ever trust Google services/products with your sensitive information. They have great control over the data and it seems their policy isn't that strict which results in taking advantage and the power of the collected data by their employees especially who have malicious intents.

At the end I need to make it clear again why I published this:

- Spread awareness among users who are using or used Coinomi wallet.
- Demand my stolen crypto-currency assets from the company behind Coinomi wallet either in terms of crypto currency or in terms of fiat currency. The more they procrastinate the more the value of the assets increase by time.
- Force Google to start investigating the issue. I'm pretty sure this is a serious issue not only in regards of my stolen crypto-currency assets but also in terms of users' privacy and their

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

data being maliciously used by Google's employees or whoever have control over these data.

Finally I hope the moderators pin this post to spread awareness. I'm pretty sure hundred thousands of crypto assets will be saved and many users will have the opportunity to save their hard earned crypto assets!

Next time if you need to spell check your passphrase/seed and to make sure that you are following the English dictionary just use Coinomi wallet LMAO!

---

peonminer
Hero Member

Activity: 798
Merit: 532

Crypto is King.

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 26, 2019, 11:55:33 PM #2

I read your whole excerpt ... this makes me sick to my stomach... RIP your life savings. I'm sorry this happened and I appreciate your detailed explanation. Glad you are documenting it all as much as possible to sue them.

I have one question....

Why did you not have a hardware wallet with the majority of your coins in there? They are like $60 USD...

---

warith (OP)
Newbie

Activity: 10
Merit: 51

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 12:16:08 AM #3
Merited by LoyceV (1)

> **Quote from: peonminer on February 26, 2019, 11:55:33 PM**
> I read your whole excerpt ... this makes me sick to my stomach... RIP your life savings. I'm sorry this happened and I appreciate your detailed explanation. Glad you are documenting it all as much as possible to sue them.
>
> I have one question....
>
> Why did you not have a hardware wallet with the majority of your coins in there? They are like $60 USD...

I'm really not sure but I think one of the reasons is that you can only have a limited number of unique coins in a single hardware (please correct if I'm wrong).

I'm used to software wallets since 2013 and never had such incident because I was taking proper security measures by isolating my crypto stuff.

Getting exploited by such stupid vulnerability was not in my list and I have learned it the hard way and hopefully the community learns from my expensive experience.

---

peonminer
Hero Member

Activity: 798
Merit: 532

Crypto is King.

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 01:15:56 AM #4

> **Quote from: warith on February 27, 2019, 12:16:08 AM**
> > **Quote from: peonminer on February 26, 2019, 11:55:33 PM**
> > I read your whole excerpt ... this makes me sick to my stomach... RIP your life savings. I'm sorry this happened and I appreciate your detailed explanation. Glad you are documenting it all as much as possible to sue them.
> >
> > I have one question....
> >
> > Why did you not have a hardware wallet with the majority of your coins in there? They are like $60 USD...

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

I'm really not sure but I think one of the reasons is that you can only have a limited number of unique coins in a single hardware (please correct if I'm wrong).

I'm used to software wallets since 2013 and never had such incident because I was taking proper security measures by isolating my crypto stuff.

Getting exploited by such stupid vulnerability was not in my list and I have learned it the hard way and hopefully the community learns from my expensive experience.

from what I understand, ledger hardware wallet can hold 1000+ coins' pub and private key so you always have your coins ready to go... I really am sorry for your loss. What a weird exploit.. man in the middle attack. The fact that coinomi threatened you with legal action... Man post this in the scam accusations sub forum. People there would have a field day looking into your claims. So basically whoever did this exploit still has access to it if I understand correctly? Everyone should pull their coinage off coinomis wallet asap. I'm a bit confused though. You said you downloaded their pgp verisigned wallet app and installed it and that's the application that is exploitable by way of spell check through Google's remote API?

---

denzkilim
Full Member

Activity: 1218
Merit: 105

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 01:38:59 AM #5

Thanks for the warning and awareness bro, and I feel sorry for your life savings that have been lost because of that wallet provider. I already quit using that Coinomi wallet a long time ago because of their bad customer support that I experienced. Losing life savings that you worked hard for it whatever price it is, is no joke I do hope that you will recover from your losses and get more blessing in the future.

> **Quote from: warith on February 26, 2019, 11:49:55 PM**
>
> As a result, someone from Google's team or whoever had access to the HTTP requests that are sent to googleapis.com found the passphrase and used it to steal my $60K-$70K worth crypto assets (at current market price). Anyone who is involved in technology and crypto-currency knows that a 12 random English words separated by spaces will probably be a passphrase to a crypto-currency wallet!

This looks really alarming Coinomi should take this kind of vulnerability seriously because the funds of their customers will be in great danger just like what happened to you.

Tamilson
Hero Member

Activity: 1022
Merit: 503

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 02:38:09 AM #6

I'm a coinomi user since 2017 and got no problem with that, so far. My biggest fund there was around $5k and didn't worry about hacking issue since I have a passphrase. But your story is different from mine since you imported your passphrase from exodus wallet and maybe someone had spotted this since you really have decent amount.

I'm not a techy person so I can't say anything, I just feel sorry for your money that seems no getting back.
And if there will further update what coinomi has to say please keep us posted here.

Happy Coding Life

---

joniboini
Legendary

Activity: 3094
Merit: 1941

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 02:55:57 AM #7

> **Quote from: Tamilson on February 27, 2019, 02:38:09 AM**
>
> But your story is different from mine since you imported your passphrase from exodus wallet and maybe someone had spotted this since you really have decent amount.

This has nothing to do with his previous passphrase/wallet. In its simplest sense, OP lost his

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

money because Coinomi has a backdoor which has been used by a hacker to get his passphrase. So whatever apps you use to generate the passphrase, you can fall for the same hack.

warith (OP)
Newbie

Activity: 10
Merit: 51

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 04:16:14 AM #8
Merited by LoyceV (2)

> **Quote from: peonminer on February 27, 2019, 01:15:56 AM**
>
> > **Quote from: warith on February 27, 2019, 12:16:08 AM**
> >
> > > **Quote from: peonminer on February 26, 2019, 11:55:33 PM**
> > >
> > > I read your whole excerpt ... this makes me sick to my stomach... RIP your life savings. I'm sorry this happened and I appreciate your detailed explanation. Glad you are documenting it all as much as possible to sue them.
> > >
> > > I have one question....
> > >
> > > Why did you not have a hardware wallet with the majority of your coins in there? They are like $60 USD...
> >
> > I'm really not sure but I think one of the reasons is that you can only have a limited number of unique coins in a single hardware (please correct if I'm wrong).
> >
> > I'm used to software wallets since 2013 and never had such incident because I was taking proper security measures by isolating my crypto stuff.
> >
> > Getting exploited by such stupid vulnerability was not in my list and I have learned it the hard way and hopefully the community learns from my expensive experience.
>
> from what I understand, ledger hardware wallet can hold 1000+ coins' pub and private key so you always have your coins ready to go... I really am sorry for your loss. What a weird exploit.. man in the middle attack. The fact that coinomi threatened you with legal action... Man post this in the scam accusations sub forum. People there would have a field day looking into your claims. So basically whoever did this exploit still has access to it if I understand correctly? Everyone should pull their coinage off coinomis wallet asap. I'm a bit confused though. You said you downloaded their pgp verisigned wallet app and installed it and that's the application that is exploitable by way of spell check through Google's remote API?

Thanks for the information and the tip.

I just wanted to point out that even hardware wallets can be vulnerable because you can't make sure that your hardware wallet does not get tampered with during shipping and someone installs predefined private keys in it. It's not about using hardware or software wallet. It's about having a well defined security policy and audit before you sell or promote your product to the end users especially when you deal with their money or crypto-currencies. At some point you have to trust the vendor otherwise and if they f***up you get f***edup too.

Regarding the access, you are right. Whoever controls googleapis.com can see your passphrase that are sent by Coinomi's wallet to them!

Companies purchase digital signatures from certificate authorities to sign their application so that when you download their application you know it's from the actual source. If anyone modifies the application (backdoors it for example) then the digital signature will be invalid. At first I thought their application was infected because it did not contain digital signature but later on I discover that they send the passphrase/seed to a remote server and that solved the puzzle.

So their signed and unsigned application are both vulnerable.

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

warith (OP)
Newbie

Activity: 10
Merit: 51

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 04:28:16 AM #9
Merited by LoyceV (1)

> **Quote from: denzkilim on February 27, 2019, 01:38:59 AM**
>
> Thanks for the warning and awareness bro, and I feel sorry for your life savings that have been lost because of that wallet provider. I already quit using that Coinomi wallet a long time ago because of their bad customer support that I experienced. Losing life savings that you worked hard for it whatever price it is, is no joke I do hope that you will recover from your losses and get more blessing in the future.
>
> > **Quote from: warith on February 26, 2019, 11:49:55 PM**
> >
> > As a result, someone from Google's team or whoever had access to the HTTP requests that are sent to googleapis.com found the passphrase and used it to steal my $60K-$70K worth crypto assets (at current market price). Anyone who is involved in technology and crypto-currency knows that a 12 random English words separated by spaces will probably be a passphrase to a crypto-currency wallet!
>
> This looks really alarming Coinomi should take this kind of vulnerability seriously because the funds of their customers will be in great danger just like what happened to you.

Yes it's totally alarming and the company behind Coinomi does not give a single f*** about the users. They patched the application without changing the version or updating the change log and they never informed their users' about the issue even after I gave them all the information they need.

warith (OP)
Newbie

Activity: 10
Merit: 51

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 04:35:00 AM #10

> **Quote from: Tamilson on February 27, 2019, 02:38:09 AM**
>
> I'm a coinomi user since 2017 and got no problem with that, so far. My biggest fund there was around $5k and didn't worry about hacking issue since I have a passphrase. But your story is different from mine since you imported your passphrase from exodus wallet and maybe someone had spotted this since you really have decent amount.
>
> I'm not a techy person so I can't say anything, I just feel sorry for your money that seems no getting back.
> And if there will further update what coinomi has to say please keep us posted here.

You probably didn't read my post very well. Coinomi's wallet simply takes your passphrase and spell checks it with a remote server!

pooya87
Legendary

Activity: 4270
Merit: 12715

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 04:38:36 AM #11

sorry about your losses, it really sucks.

i have never used any wallet on my phone so i don't really check these things but interestingly enough coinomi GitHub doesn't seem to be updated for more than 2 months[1] which makes me wonder whether their wallet is even open source because that is the first thing i checked after reading your topic, i wanted to see where the bug was and whether it was fixed or not (specially since this type of bug is so weird and obvious!). it seems like they have released a new version (yesterday) on google play but nothing is happening on their github.
comparing with other wallets (Electrum, Breadwallet, Mycelium, Samourai,...) they all are actively updating the source code and you can even compile it from source yourself.

[1] https://github.com/Coinomi/coinomi-android

DEX.fo
NO HIDDEN FEES ❯❯ NO LOGS ❯❯ NO REGISTRATION
AUTOMATIC CRYPTO EXCHANGE
NO KYC

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

warith (OP)
Newbie

Activity: 10
Merit: 51

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 04:53:48 AM #12
Merited by LoyceV (1)

> **Quote from: pooya87 on February 27, 2019, 04:38:36 AM**
> sorry about your losses, it really sucks.
>
> i have never used any wallet on my phone so i don't really check these things but interestingly enough coinomi GitHub doesn't seem to be updated for more than 2 months[1] which makes me wonder whether their wallet is even open source because that is the first thing i checked after reading your topic, i wanted to see where the bug was and whether it was fixed or not (specially since this type of bug is so weird and obvious!). it seems like they have released a new version (yesterday) on google play but nothing is happening on their github. comparing with other wallets (Electrum, Breadwallet, Mycelium, Samourai,...) they all are actively updating the source code and you can even compile it from source yourself.
>
> [1] https://github.com/Coinomi/coinomi-android

They claim opensource but in reality their application is not opensource. Github account is inactive and they admitted that. Read the following links+comments (these are old articles/posts but it confirms the opensource thing):
https://bitsonline.com/coinomi-vulnerability-respond/
https://imnotdead.co.uk/blog/coinomi

peonminer
Hero Member

Activity: 798
Merit: 532

Crypto is King.

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 04:55:37 AM #13

> **Quote from: warith on February 27, 2019, 04:16:14 AM**
> **Quote from: peonminer on February 27, 2019, 01:15:56 AM**
> **Quote from: warith on February 27, 2019, 12:16:08 AM**
> **Quote from: peonminer on February 26, 2019, 11:55:33 PM**
> I read your whole excerpt ... this makes me sick to my stomach... RIP your life savings. I'm sorry this happened and I appreciate your detailed explanation. Glad you are documenting it all as much as possible to sue them.
>
> I have one question....
>
> Why did you not have a hardware wallet with the majority of your coins in there? They are like $60 USD...
>
> I'm really not sure but I think one of the reasons is that you can only have a limited number of unique coins in a single hardware (please correct if I'm wrong).
>
> I'm used to software wallets since 2013 and never had such incident because I was taking proper security measures by isolating my crypto stuff.
>
> Getting exploited by such stupid vulnerability was not in my list and I have learned it the hard way and hopefully the community learns from my expensive experience.
>
> from what I understand, ledger hardware wallet can hold 1000+ coins' pub and private key so you always have your coins ready to go... I really am sorry for your loss. What a weird exploit.. man in the middle attack. The fact that coinomi threatened you with legal action... Man post this in the scam accusations sub forum. People there would have a field day looking into your claims. So basically whoever did this exploit still has access to it if I understand correctly? Everyone should pull their coinage off coinomis wallet asap. I'm a bit confused though. You said you downloaded their pgp verisigned wallet app and installed it and that's the application that is exploitable by way of spell check through Google's remote API?

Thanks for the information and the tip.

I just wanted to point out that even hardware wallets can be vulnerable because you can't make sure that your hardware wallet does not get tampered with during shipping and someone installs predefined private keys in it.

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

> It's not about using hardware or software wallet. It's about having a well defined security policy and audit before you sell or promote your product to the end users especially when you deal with their money or crypto-currencies. At some point you have to trust the vendor otherwise and if they f***up you get f***edup too.
>
> Regarding the access, you are right. Whoever controls googleapis.com can see your passphrase that are sent by Coinomi's wallet to them!
>
> Companies purchase digital signatures from certificate authorities to sign their application so that when you download their application you know it's from the actual source. If anyone modifies the application (backdoors it for example) then the digital signature will be invalid. At first I thought their application was infected because it did not contain digital signature but later on I discover that they send the passphrase/seed to a remote server and that solved the puzzle.
>
> So their signed and unsigned application are both vulnerable.

damn you are right about the fact that they could preload the wallets with a backdoor from shipping a hard wallet... never thought about it like that... ffs that worries me lol. I'm going to do much more digging on hardware wallets now before I decide on one.

In regards to the man in the middle attack that got you... HFS man. Someone who works for a Google entity swiped you... what a shame. I wonder how many other people have suffered from this exploit... now that it is released into the light web it'll probably be replicated by other means at a higher rate... users beware please.

Did you have a passphrase set on your wallet to send and receive or just the seed code to recover the pub/priv keys? Reason why I ask is I am curious if you have a password on your wallet.dat and someone is able to type in your seed string, would they still be able to steal your coins without the wallet passphrase?

---

warith (OP)
Newbie

Activity: 10
Merit: 51

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

February 27, 2019, 05:17:49 AM
Merited by LoyceV (1)

#14

> **Quote from: peonminer on February 27, 2019, 04:55:37 AM**
>
> > **Quote from: warith on February 27, 2019, 04:16:14 AM**
> >
> > > **Quote from: peonminer on February 27, 2019, 01:15:56 AM**
> > >
> > > > **Quote from: warith on February 27, 2019, 12:16:08 AM**
> > > >
> > > > > **Quote from: peonminer on February 26, 2019, 11:55:33 PM**
> > > > >
> > > > > > I read your whole excerpt ... this makes me sick to my stomach... RIP your life savings. I'm sorry this happened and I appreciate your detailed explanation. Glad you are documenting it all as much as possible to sue them.
> > > > > >
> > > > > > I have one question....
> > > > > >
> > > > > > Why did you not have a hardware wallet with the majority of your coins in there? They are like $60 USD...
> > > > >
> > > > > I'm really not sure but I think one of the reasons is that you can only have a limited number of unique coins in a single hardware (please correct if I'm wrong).
> > > > >
> > > > > I'm used to software wallets since 2013 and never had such incident because I was taking proper security measures by isolating my crypto stuff.
> > > > >
> > > > > Getting exploited by such stupid vulnerability was not in my list and I have learned it the hard way and hopefully the community learns from my expensive experience.
> > > >
> > > > from what I understand, ledger hardware wallet can hold 1000+ coins' pub and private key so you always have your coins ready to go... I really am sorry for your loss. What a weird exploit.. man in the middle attack. The fact that coinomi threatened you with legal action... Man post this in the scam accusations sub forum. People there would have a field day looking into your claims. So basically whoever did this exploit still has access to it if I understand correctly? Everyone should pull their coinage off coinomis wallet asap. I'm a bit confused though. You said you downloaded their pgp

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

> verisigned wallet app and installed it and that's the application that is exploitable by way of spell check through Google's remote API?

Thanks for the information and the tip.

I just wanted to point out that even hardware wallets can be vulnerable because you can't make sure that your hardware wallet does not get tampered with during shipping and someone installs predefined private keys in it. It's not about using hardware or software wallet. It's about having a well defined security policy and audit before you sell or promote your product to the end users especially when you deal with their money or crypto-currencies. At some point you have to trust the vendor otherwise and if they f***up you get f***edup too.

Regarding the access, you are right. Whoever controls googleapis.com can see your passphrase that are sent by Coinomi's wallet to them!

Companies purchase digital signatures from certificate authorities to sign their application so that when you download their application you know it's from the actual source. If anyone modifies the application (backdoors it for example) then the digital signature will be invalid. At first I thought their application was infected because it did not contain digital signature but later on I discover that they send the passphrase/seed to a remote server and that solved the puzzle.

So their signed and unsigned application are both vulnerable.

damn you are right about the fact that they could preload the wallets with a backdoor from shipping a hard wallet... never thought about it like that... ffs that worries me lol. I'm going to do much more digging on hardware wallets now before I decide on one.

In regards to the man in the middle attack that got you... HFS man. Someone who works for a Google entity swiped you... what a shame. I wonder how many other people have suffered from this exploit... now that it is released into the light web it'll probably be replicated by other means at a higher rate... users beware please.

Did you have a passphrase set on your wallet to send and receive or just the seed code to recover the pub/priv keys? Reason why I ask is I am curious if you have a password on your wallet.dat and someone is able to type in your seed string, would they still be able to steal your coins without the wallet passphrase?

Apparently I'm not the only one who got wiped out check these reddit posts:
https://www.reddit.com/r/COINOMI/comments/av8rp0/was_i_hacked_im_not_sure_what_i_did_wr
https://www.reddit.com/r/COINOMI/comments/av01oz/coinnomi_hacked/
https://www.reddit.com/r/CryptoCurrency/comments/9cja43/half_my_coins_are_missing_from_ver

This proves my analysis but yet the company denies the responsibility.

What I did was I used one of my main wallets passphrase/seed (recovery seed) in Coinomi's wallet and that was my awful mistake! If it was the password that protect the private key (wallet.dat) then the attacker/criminal would not be able to do anything because he must obtain the private key in order to use the password and steal the wallet.

Kakmakr
Legendary

Activity: 3542
Merit: 1966

Leading Crypto Sports Betting & Casino Platform

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings

#15

February 27, 2019, 05:28:00 AM

What I do not understand is, why Coinomi need to spell check your seed phrase on googleapis.com? Is this done on purpose to blame external factors, when someone within the company used this "backdoor" and get caught?

I have always said that centralized wallet providers and exchanges should never be trusted with your life savings. DO NOT put all your eggs in one basket. <80%+ of my hoard are stored on Cold wallets & Hardware wallets and only 20% are stored on different centralized services for daily access>

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

Stake.com Play Smarter Leading Crypto Sports PLAY

Tamilson
Hero Member

Activity: 1022
Merit: 503

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings
February 27, 2019, 05:56:43 AM #16

> **Quote from: warith on February 27, 2019, 04:35:00 AM**
>
> > **Quote from: Tamilson on February 27, 2019, 02:38:09 AM**
> >
> > I'm a coinomi user since 2017 and got no problem with that, so far. My biggest fund there was around $5k and didn't worry about hacking issue since I have a passphrase. But your story is different from mine since you imported your passphrase from exodus wallet and maybe someone had spotted this since you really have decent amount.
> >
> > I'm not a techy person so I can't say anything, I just feel sorry for your money that seems no getting back. And if there will further update what coinomi has to say please keep us posted here.
>
> You probably didn't read my post very well. Coinomi's wallet simply takes your passphrase and spell checks it with a remote server!

Sort of since it's lengthy, lol. Well I really thought that it's exodus the importing that triggered everything, pardon me on that. So earlier, had checked those links in the OP since honestly I'm in coinomi's side (sorry again) but upon reading all those links I found out these are all true (especially those reddit posts). Maybe I trusted it too much and ain't aware those "backdoors".

I'm having my thoughts right now which wallets are safe since even a hardware wallet can be tampered upon shipping.

Happy Coding Life

maydna
Hero Member

Activity: 3808
Merit: 588

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings
February 27, 2019, 06:25:46 AM #17
Merited by *DdmrDdmr* *(2)*

My big question is why you use Coinomi to safe your asset worth $60K-$70K? It doesn't make sense for me. With so much money inside the wallet, you can buy hardware wallet like Ledger S Nano even Ledger X Nano (which is the newest product from Ledger). I don't want to get any trouble to save all of my asset in the wallet online or offline.

You can buy 10 or even more Ledger X Nano to save all of your assets. The first mistake is because of yourself, and you do not realize about that, and now, you got the trouble for losing all of the assets because Coinomi compromised your passphrase. It's not about their mistake to get inside your wallet, but it's our responsibility to protect all of we had. Realize that thing first.

I think your computer was compromised with malware because you use Windows wallet installer which you don't know is it safe or not. But once again, next time if you have an asset worth for $1k or more, it is better you save it in the Ledger or Trezor.

Personally, I use Coinomi wallet to in my android phone, but I don't save all the asset inside the wallet, and I only save for 5-10 coins in there. The rest coin, I keep it in my ledger. I don't have any trouble so far.

It is an important lesson for you and for every people who have a large asset, never used a wallet in online or inside the computer, it is better to buy one hardware wallet which can save all of the assets so you don't have to worry about something bad that might happen.

davis196
Hero Member

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings
February 27, 2019, 06:27:48 AM #18

Captured 2026-10-30T07:28:46.437Z from https://bitcointalk.org/index.php?topic=5114708.0

Activity: 3850
Merit: 980

I've never heard about this Coinomi wallet.Why didn't you just use one of the more popular and trusted crypto wallet services?Storing big amounts of coins into ONE wallet is always a big mistake...
This topic belongs to the Scam Acusasations forums,I think...

CCC.io - Crypto Casino & Web3 Betting Platform

jseverson
Hero Member

Activity: 1834
Merit: 759

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings #19
February 27, 2019, 06:29:23 AM

Those are some pretty damning evidence. If I had money in a Coinomi Wallet, I'd be sweating bullets as I transfer my funds right about now. I mean, transferring data in plaintext is one thing, but are you sure some random Google employee was able to see your seed? Wouldn't they have strict protocols to avoid scenarios like that? Maybe your traffic was intercepted or something.

But yeah I suppose that's not the main issue. This is yet another harsh reminder to trust no one.

As an addendum, I hope something comes out of your legal action. Pretty much every single wallet out there state that they won't be responsible for any losses on their ToS that they make you agree to. It's going to be an uphill battle.

himanshuoe
Jr. Member

Activity: 45
Merit: 12

Re: WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings #20
February 27, 2019, 06:33:33 AM

What a sad and pathetic thing to read.

As if these exit scams were not enough , now even companies doing so.

I m fed up of these scams.

May Ur steps end these incidents for ever.

Best luck.

Pages: [1] 2 3 4 5 6 » All

print

« previous topic next topic »

Bitcoin Forum > Bitcoin > Bitcoin Discussion > **WARNING - Coinomi Wallet CRITICAL Vulnerability Made Me Lose My Life Savings**

Jump to: => Bitcoin Discussion go

Powered by SMF 1.1.19 | SMF © 2006-2009, Simple Machines