

Forum:[Hack Forums](#)

Thread: [Windows 10 NSA announces flaw - update now if you use OS](#)

Mr. Robot - January 15, 2020, 5:24 pm

<https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/>

Quote:In a shift toward transparency, the National Security Agency announced a bug that could have left over 900 million PCs vulnerable to attack.

Long story short it's being called the "Windows 10 validation bug" which is exactly what i've talked about on here before. I'm not trying to take credit for inspiring the attack however it's pretty clear and obvious how it happens.

I theorized a while back that you could break the certification of a windows update or any program update with an infected file, even as far as in some cases - having someones IP address and knowing what programs they run, pinging an application for an update and infecting the update with a malicious file.

While this NSA report is specifically for Windows 10 as the base OS itself, it's still a heavy possibility to do this through other applications you have installed on your machine. Always be careful of what you install and allow automatic updates for.

<https://twitter.com/NSAGov>

<https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF>

Quote:NSA has discovered a critical vulnerability (CVE-2020-0601) affecting Microsoft Windows® cryptographic functionality.

The certificate validation vulnerability allows an attacker to undermine how Windows verifies cryptographic trust and can

enable remote code execution. The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as

applications that rely on Windows for trust functionality. Exploitation of the vulnerability allows attackers to defeat trusted

network connections and deliver executable code while appearing as legitimately trusted entities.

Examples where

validation of trust may be impacted include

If you want it dumbed down a bit - they put out this also which touches on other applications being used in this way.

Quote:CVE-2020-0601 is a serious vulnerability, because it can be exploited to undermine Public Key Infrastructure (PKI) trust. PKI is a set of mechanisms that home users, businesses, and governments rely upon in a wide variety of ways. The vulnerability permits an attacker to craft PKI certificates to spoof trusted identifies, such as individuals, web sites, software companies, service providers, or others. Using a forged certificate, the attacker can (under certain conditions) gain the trust of users or services on vulnerable systems, and leverage that trust to compromise them.

//

For those wondering, here is one example of the many threads I made on it - this one is about 4 months ago.

<https://hackforums.net/showthread.php?tid=5987664>

Quote:I'm not quite sure how this would play out yet as I assume most paths are clearly patched.

Say a program like Chrome is installed and we can see that through a man in the middle attack (headers).

We see an update for the browser has been released or just about to be released that day.

What if we grab that certificate for the browser update and craft a malicious replacement for the man in the middle attack.

Same would apply for Windows or Adobe applications - surely there must be something that's vulnerable through that. I haven't personally seen anyone doing network exploitation through application updates before.

Charger - January 15, 2020, 5:50 pm

Tbh I don't believe anything unless a PoC is provided. Probably just me.

Mr. Robot - January 15, 2020, 5:52 pm

(Jan 15, 2020 06:50 PM)Charger Wrote: [\[CITE\]](#) Tbh I don't believe anything unless a PoC is provided. Probably just me.

I think that's a very dangerous way to live lmao - like 99% of known attacks online don't have proof of concept attached.

Also there are about 10 private POCs for this out there.

Lorem Ipsum - January 16, 2020, 5:45 am

Isn't it true that the NSA itself installed some 'files' at our computers in order to monitor it?

I heard about such release a few years ago at a different forum, claiming to have found the weird file extensions of the NSA 'spyware'. Just rumours, I can't verify anything.

Mr. Robot - January 16, 2020, 5:51 am

(Jan 16, 2020 06:45 AM)Lorem Ipsum Wrote: [\[CITE\]](#) Isn't it true that the NSA itself installed some 'files' at our computers in order to monitor it?

I heard about such release a few years ago at a different forum, claiming to have found the weird file extensions of the NSA 'spyware'. Just rumours, I can't verify anything.

Yeah like notepad++ they had backdoors for. Heaps of shit.

Lorem Ipsum - January 16, 2020, 5:52 am

(Jan 16, 2020 06:51 AM)Mr. Robot Wrote: [\[CITE\]](#) Yeah like notepad++ they had backdoors for. Heaps of Clay Davis.

I used Notepad++ in the past for HTML editing. Glad I switched to Mac OS although I use Windows occasionally too.

What is the best anti-virus software in your opinion? Or how do you protect yourself against the Windows 10 'flaws'.

Btw, pretty ironic. First disabling Windows XP from updates, then making Windows 8 and free update to Windows 10 and now they figured out it has flaws? Sounds weird to me.

Mr. Robot - January 16, 2020, 5:56 am

(Jan 16, 2020 06:52 AM)Lorem Ipsum Wrote: [\[CITE\]](#) I used Notepad++ in the past for HTML editing. Glad I switched to Mac OS although I use Windows occasionally too.

What is the best anti-virus software in your opinion? Or how do you protect yourself against the Windows 10 'flaws'.

Btw, pretty ironic. First disabling Windows XP from updates, then making Windows 8 and free update to Windows 10 and now they figured out it has flaws? Sounds weird to me.

Well yes and no but overall it's important to remember exploits will always be found - whether intentional or not, not all of them were intended.

Honestly you don't. You just do whatever you can network side and then keep track of incoming and outgoing connections. You will never have time to analyze every single packet of data that leaves but you can learn to identify the interesting ones.

When it comes to the NSA, any data that microsoft sees will go there so it's like w/e - the main issue is the people on HF talking shit about how their system is running linux or some shit then realize oh wait people who use the same network as me use windows...

Stoopd af

Lorem Ipsum - January 16, 2020, 5:59 am

(Jan 16, 2020 06:56 AM)Mr. Robot Wrote: [\[CITE\]](#) Well yes and no but overall it's important to remember exploits will always be found - whether intentional or not, not all of them were intended.

Honestly you don't. You just do whatever you can network side and then keep track of incoming and outgoing connections. You will never have time to analyze every single packet of data that leaves but you can learn to identify the interesting ones.

When it comes to the NSA, any data that microsoft sees will go there so it's like w/e - the main issue is the people on HF talking Clay Davis about how their system is running linux or some Clay Davis then realize oh wait people who use the same network as me use windows...

Stoopd af

I think the majority of people, not only at HF, but in general, feel 'safe' while browsing online without having any clue why they aren't safe.

The privacy of online usage isn't what it was, nor will it ever become any better I think. Just trying to stay as safe as possible here. ?

Mr. Robot - January 16, 2020, 6:00 am

(Jan 16, 2020 06:59 AM)Lorem Ipsum Wrote: [\[CITE\]](#) I think the majority of people, not only at HF, but in general, feel 'safe' while browsing online without having any clue why they aren't safe.

The privacy of online usage isn't what it was, nor will it ever become any better I think. Just trying to stay as safe as possible here. ?

One day we will have AI hacking and AI defense. Battling it out, making us more secure.

Lorem Ipsum - January 16, 2020, 6:04 am

(Jan 16, 2020 07:00 AM)Mr. Robot Wrote: [\[CITE\]](#) One day we will have AI hacking and AI defense. Battling it out, making us more secure.

I honestly fear the day that AI is trying to take over. They killed 20 Japanese inventors and scientists (Asian either way) was enough proof to me that it already started. Due to video gaming, Alexa and other devices they are trying to make us feel 'common' to talk to robots.

That way it's easier to implement AI all over the world once the timing is right. Just my thoughts though.

hayesh - January 16, 2020, 7:01 am

Since when has the NSA cared about protecting peoples privacy

AmazingLicense - January 16, 2020, 7:15 am

(Jan 16, 2020 08:01 AM)hayesh Wrote: [\[CITE\]](#) Since when has the NSA cared about protecting peoples privacy

Exactly.

I think there is something to this update that NSA benefits...