

Forum:[Hack Forums](#)

Thread: [\[VPN USERS: \]>_ Your VPN could be Leaking your REAL IP Address _\[/How to fix\]](#)

mObile - February 12, 2015, 3:43 pm

A new security flaw can reveal your real IP address to prying eyes, even if you're using a VPN, and it's easy to exploit. Here's how it works, and what you can do about it. A recently discovered security flaw allows remote sites to take advantage of WebRTC (Web Real Time Communication, a feature built in to most browsers.

A few lines of code is all it takes to remove the location protection you get from using a VPN, and figure out where you're actually located and who your internet service provider really is (who can then tie your address back to who you are specifically.) While the vulnerability is primarily browser-based right now, any application that can render web pages (and uses WebRTC) is affected, meaning anyone who wants to can see past your VPN to where you really are and who you really are. Advertisers, data brokers, and governments can use it to peek through your VPN to find out where your connection is really coming from.

How Can I Check If My VPN Is Affected?

Firefox and Chrome have implemented WebRTC that allow requests to STUN servers be made that will return the local and public IP addresses for the user. These request results are available to javascript, so you can now obtain a users local and public IP addresses in javascript. This demo is an example implementation of that.

Additionally, these STUN requests are made outside of the normal XMLHttpRequest procedure, so they are not visible in the developer console or able to be blocked by plugins such as AdblockPlus or Ghostery. This makes these types of requests available for online tracking if an advertiser sets up a STUN server with a wildcard domain.

To see if your VPN is affected:

1.) Visit:

Quote:<http://whatismyipaddress.com/>

and jot down your actual ISP-provided IP address.

2.) Log in to your VPN, choose an exit server in another country (or use whichever exit server you prefer) and verify you're connected.

3.) Go back to What Is My IP Address and check your IP address again. You should see a new address, one that corresponds with your VPN and the country you selected.

4.) Visit Roseler's WebRTC test page

Quote:<https://diafygi.github.io/webrtc-ips/>

and note the IP address displayed on the page.

[img]http://torrentfreak.com/images/nkoreaip.png[/img]

If both tools show your VPN's IP address, then you're in the clear. However, if What Is My IP Address shows your VPN and the WebRTC test shows your normal IP address, then your browser is leaking your ISP-provided address to the world.

The Easy Way: Disable WebRTC In Your Browser.

Chrome, Firefox, and Opera (and browsers based on them) generally have WebRTC enabled by default. Safari and Internet Explorer don't, and thus aren't affected (unless you've specifically enabled WebRTC.) Either way, if the test above worked in your browser, you're affected. You can always switch to a browser that doesn't have WebRTC enabled, but since most of us like the browsers we use, here's what to do:

Chrome and Opera:

Install RTC Block or ScriptSafe extension from the Chrome Web Store. It's overkill, but it'll disable WebRTC in your browser.

Quote:

<https://chrome.google.com/webstore/detail/webrtc-block/nphkkbaidamjmhfanlpblblcadhfbkdm?hl=en>

Quote:

<https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijflahbdbdgdf?hl=en>

Firefox: You have two options. You can install the Disable WebRTC addon from Mozilla Add-ons

Quote: <https://addons.mozilla.org/en-US/firefox/addon/happy-bonobo-disable-webrtc/>

or disable WebRTC directly by opening a tab and going to

PHP Code

<?php

about:config

in the address bar. Find and set the

PHP Code

<?php

media.peerconnection.enabled

setting to false.

To be sure WebRTC is disabled go to:

Quote: <https://www.browserleaks.com/webrtc>

and you should see something like this, if your good.

Otherwise you will see this:

I know a lot of you use VPN software and probably don't know about this so I hope it was helpful. Got to stay anonymous if you are hacking websites, ? ?

SOURCES:

Spoiler ([Click to View](#))

PHP Code

<?php

<http://torrentfreak.com/huge-security-flaw-leaks-vpn-users-real-ip-addresses-150130/>

PHP Code

<?php

<http://lifehacker.com/how-to-see-if-your-vpn-is-leaking-your-ip-address-and-1685180082>

PHP Code

<?php

<https://www.browserleaks.com/webrtc>

FRANKIE - February 12, 2015, 3:44 pm

I believe this was posted about earlier but for those that were not able to see it I am sure they will thank you.

Zealot - February 12, 2015, 6:00 pm

I did not know this at all, thanks man.

Suits - February 12, 2015, 6:01 pm

A++ man. Great info on taking proper precautions with VPNs.

Inkling - February 12, 2015, 6:03 pm

Check out my signature to abuse this bug with my IP Logger. :)

robby_j - February 12, 2015, 7:26 pm

This is false. Only proxy servers would be affected by this.

Scy7e - February 12, 2015, 7:33 pm

(Feb 12, 2015 08:26 PM)cl0ck Wrote: [\[CITE\]](#) This is false. Only proxy servers would be affected by this.

This is not false at all. It definitely is able to get your real IP even from behind a Tor as long as webRTC isn't disabled. I've used this exploit for quite a while now and it has worked more often than not.

EPIXIA???? - February 12, 2015, 7:51 pm

(Feb 12, 2015 08:33 PM)Scy7e Wrote: [\[CITE\]](#) It definitely is able to get your real IP even from behind a Tor as long as webRTC isn't disabled.webRTC is disabled by default in Tor already

(Feb 12, 2015 07:03 PM)Inkling Wrote: [\[CITE\]](#) Check out my signature to abuse this bug with my IP Logger. :)[This is not a bug, it is by design](#)

Scy7e - February 12, 2015, 8:05 pm

(Feb 12, 2015 08:51 PM)EPIXIA????? Wrote: [\[CITE\]](#) webRTC is disabled by default in Tor already
Yes, on the official client, though I don't see many reasons why someone would use anything else.
Either way, works almost 10/10 on VPN.

Jcgob - February 12, 2015, 8:20 pm

I think Internet Explore won this battle ;)

frank3nstien - February 12, 2015, 11:09 pm

Thank you for these TUT, I will Check it now with my Premium VPN ?

robby_j - February 12, 2015, 11:19 pm

(Feb 12, 2015 08:33 PM)Scy7e Wrote: [\[CITE\]](#) This is not false at all. It definitely is able to get your real IP even from behind a Tor as long as webRTC isn't disabled. I've used this exploit for quite a while now and it has worked more often than not. Tor isn't a VPN. Free VPN's even block this.

Scy7e - February 12, 2015, 11:34 pm

(Feb 13, 2015 12:19 AM)cl0ck Wrote: [\[CITE\]](#) Tor isn't a VPN. Free VPN's even block this.

I never said Tor is a VPN. I don't know what kind of point you're trying to make, the fact is this exploit does work as long as webRTC isn't disabled, be it a VPN or Tor. Not all VPN's block this and neither does Tor in some edge cases.

Frankstare - February 13, 2015, 12:34 am

Thanks for posting about this, wouldn't have known if I didn't see this.

Chr0nicHax - February 13, 2015, 4:24 am

<http://nexon-nx.ml/iplogger/js/x01.js>

[JS_Kryptik.ALB trojan](#)

this is the only source on that page:

```
<script src="js/x01.js"></script>
```

Benign - February 13, 2015, 5:21 am

(Feb 13, 2015 12:34 AM)Scy7e Wrote: [\[CITE\]](#) I never said Tor is a VPN. I don't know what kind of point you're trying to make, the fact is this exploit does work as long as webRTC isn't disabled, be it a VPN or Tor. Not all VPN's block this and neither does Tor in some edge cases.

I think the point being made is that tor is a proxy. This leak only affects proxies where you have configured only one port/protocol (for example web) as you may browse to a site and it appears you are connecting from the proxy but when a different port or protocol is requested it may bypass the proxy as you have not configured it to proxy those ports. A VPN by it's very nature tunnels all traffic no matter what protocol or port through the VPN and so info leaks like this are not relevant.

It's similar to the JavaScript IP leak.

uberalles - February 13, 2015, 5:44 am

Thanks for posting this.

(35 chars)

Wireless Network - February 13, 2015, 6:57 am

Thanks for share bro. Very helpful..

robby_j - February 13, 2015, 2:25 pm

(Feb 13, 2015 12:34 AM)Scy7e Wrote: [\[CITE\]](#) I never said Tor is a VPN. I don't know what kind of point you're trying to make, the fact is this exploit does work as long as webRTC isn't disabled, be it a VPN or Tor. Not all VPN's block this and neither does Tor in some edge cases. My point is. That is false. If you are using a VPN. (Which you implied Tor was and it isn't. See post #7) This exploit will

not work.

77jefferies - February 14, 2015, 8:35 am

Thanks that is useful to know.

There is also DNS leak you can check that hear <http://ipleak.net>

Zbiniew - April 28, 2015, 6:50 am

thanks for this, I knew some VPN could possibly leak IP but I didn't know how it was done and how to prevent it

usefull informations here

#Skyline - April 28, 2015, 6:26 pm

This is a great tutorial.

Thanks for this, it will could in handy.

knightserv - April 29, 2015, 9:57 pm

thank you very much for all the info thank for looking out...

Inkling - April 29, 2015, 9:59 pm

Thanks for this. I also have a thread about my IP Logger that utilizes these IP Leaks.

Keep yourself safe.

#Windows10 - April 29, 2015, 10:22 pm

thanks for this guide, i tested my chrome using vpn and it doesnt show my real ip.

i guess im secure enough :)

TheWeeknd.. - April 30, 2015, 2:58 am

Before I even do anything I looked at WebRTC and it was already disabled so I guess I'm good.

Mcbride - April 30, 2015, 3:32 am

I could only fix this on Firefox, thanks for the information on Google chrome fix.

Grimeta - May 2, 2015, 4:55 am

This info should be a sticky somewhere. A must-know thing. Thank you for this.

BrokenMachine99 - May 11, 2015, 11:35 am

nice thread man keep it up.ssssss

eMblaze - May 11, 2015, 1:42 pm

That's why all of us use tor browser I think...

ROFL OMG - May 11, 2015, 4:43 pm

Was using "Private Internet ACESS" VPN and it leaked my real ip. Great thread and I fixed the issue now:)

A+++

Zeroxal - May 12, 2015, 7:56 am

Thanks for the share!

However I dont get any IP adress with the WebRCT test. It just leaves the Ip adress blank. But on Whatsmyip it shows the vpn address. Please help

BenkaTv - May 12, 2015, 11:52 am

Thanks for the share i will check it now!

xc0der - October 25, 2015, 1:04 am

Thank you for the share great

SIM-2875347 - October 26, 2015, 12:32 pm

Thanks a lot man turns out I could have been found

Cenu - February 6, 2016, 5:40 am

nice! didn't knew this

rgds

hakler - March 12, 2016, 8:05 pm

Thank you very much.Great info

Username is already taken - March 14, 2016, 3:24 am

Excellent thread. Thanks for bringing this security and privacy issue to the attention of the HackForums community. A++ tutorial, kudos to you.

Sh4rk Seny - March 15, 2016, 10:23 am

Thanks for sharing, I didnt expect that still using VPN the real ip still visible

myownlogs11 - March 22, 2016, 8:59 am

the best vpn ever since, when i was usng it

Çh+?melÉon - March 23, 2016, 12:04 am

Thank you, did not know about this. You saved my future. Gonna upgrade soon and you are the first person I'm going to rep :):):)

Ronaldo. - March 23, 2016, 10:25 am

Thanks for sharing.

Will check this as soon as I get back to my PC.

RainSpider3000 - March 23, 2016, 10:27 am

This stuff is broken. All it says is:

Demo for: <https://github.com/diafygi/webrtc-ips>

This demo secretly makes requests to STUN servers that can log your request. These requests do not show up in developer consoles and cannot be blocked by browser plugins (AdBlock, Ghostery, etc.).

Your local IP addresses:

Your public IP addresses:

Your IPv6 addresses:

-Tab- - April 6, 2016, 4:40 am

Great thank you for the info I will check it with my VPN's its an interesting test cause from what i saw most of the test don't see my vpn

Mekkay - April 8, 2016, 5:43 am

thank you guys I wish you continued success :)

sub7- - April 8, 2016, 5:47 am

this is one question for you. How come when I infect myself and then I see myself in my RAT.... it shows my real IP there.... even though I am using a VPN and checked for leaks already.

Caliban - April 8, 2016, 6:08 am

Nice info thanks OP. Just got the extension

banc1234 - April 9, 2016, 12:27 am

VPN --- i must say that if you are connecting to vpn each time than you are fucked because they will now which vpn you are connecting to ... so please use reaver and connect to wireless and than use vpn... or always use vpn in your router settings ... have a nice day !

BalmungOfTheAzurySky - April 23, 2016, 2:38 am

Great post man really helpfull

denielsmith - April 23, 2016, 2:41 am

I did not know this at all, thanks man.

bwfcwalshy - April 23, 2016, 3:11 am

Well done! This is a very good and informative post.

The Kraken - April 23, 2016, 3:28 am

Thanks for the post man,
luckily RA4W VPN is trusted and doesn't leak your real ip-adress.
Big vouch to RA4W VPN!

Elgordobastardo1 - April 25, 2016, 7:46 pm

Very nice info! Thank you.

?Citizen Z / Napalm - April 27, 2016, 6:33 am

Don't forget DNS Leaks, DNS leaks aswell as WebRTC

TheChi?f - November 23, 2016, 9:08 pm

Thanks a lot for this tutorial, m0bile.

InjectOG - November 24, 2016, 8:25 pm

Interesting, thanks for the share OP.

XmysteriousX - January 22, 2017, 4:45 pm

wow i didnt know this thanks a lot bro

Define© - January 23, 2017, 7:58 pm

IPv6 can sometimes be an issue too.

cz3kit - January 24, 2017, 4:53 pm

Thanks for the information. I will definitely check that out :)

GodRyuk - January 25, 2017, 1:53 am

I think Internet Explore won this battle ;) Haha

Disparity - January 25, 2017, 2:00 am

(Apr 23, 2016 03:28 AM)TechBear Wrote: [\[CITE\]](#) Thanks for the post man, luckily RA4W VPN is trusted and doesn't leak your real ip-adress. Big vouch to RA4W VPN! Um, that's not how this works.

LordDragon - September 19, 2018, 9:14 am

Wow thanks very much for this post,will try this.

Lextian - May 2, 2019, 5:17 pm

Thanks for the post, very helpful details since i had no ideal about this ip leak.

codezedd - November 15, 2019, 2:16 pm

Please add this to your post...

To disable Media Devices, "toggle media.navigator.enabled" as well as "media.peerconnection.enabled" both to FALSE.

Aghora - November 16, 2019, 10:14 pm

It dosent show anything for me on 2nd website. what does that mean ?

SlowMehMo - November 18, 2019, 12:05 am

(Nov 16, 2019 11:14 PM)Aghora Wrote: [\[CITE\]](#) It dosent show anything for me on 2nd website. what does that mean ?

that site dont work anymore, try this one 2ip.io/privacy