

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to check if VPN revealing your original IP or not](#)

frank3nstien - June 15, 2020, 8:02 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

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

and Note down your actual ISP-provided IP address.

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

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.

Visit Roseler's WebRTC test page

Spoiler ([Click to View](#))

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.

[webrtc-block](#)
[scriptsafe](#)

Firefox:

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

[happy-bonobo-disable-webrtc](#)

OR disable WebRTC directly by opening a tab and go to :

PHP Code

```
<?php
```

```
about:config
```

```
// in the address bar Find and set the
```

```
media.peerconnection.enabled
```

```
// setting to false.
```

Spoiler [\(Click to View\)](#)

To be sure WebRTC is disabled go to:

[Webrtc Leaks Check](#)

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

Spoiler [\(Click to View\)](#)

Otherwise you will see this:

Spoiler [\(Click to View\)](#)

765F - June 18, 2020, 11:38 am

Great stuff. Thank you for the information provided @frank3nstien