

Using HotSpot Shield for security or Facebook access? Your IP is at risk of being exposed

And not only the HotSpot Shield alone, but also the PureVPN and Zenmate.

Researchers have found a serious vulnerability that could leak true IP addresses and other sensitive information on very popular and widely used VPN software.

1. VPN theory - What is a virtual private network?
2. Useful virtual private networks on Google Chrome

Some people use VPN to browse anonymously or to protect their identity, and many people use them to hide their real IP addresses, bypass censorship and access blocked websites by region. But the bad news is that these software reveal the information you want to hide.

A group of three hackers hired by Mentor VPN revealed that three very popular VPN service providers, the HotSpot Shield, the PureVPN and the Zenmate - with millions of users around the world - turned out to be vulnerable.

After some security tests on these 3 VPN services, the team found that all three leaked the user's real IP, thereby identifying their identity and location.

The PureVPN is also the company that says it has never recorded history, but a few months ago used access history to help the FBI arrest a man in online surveillance.

The issue of Zenmate and PureVPN has not been published in detail because it has not been patched yet, but VPN Mentor said the error on Zenmate is less serious than the HotSpot Shield and PureVPN.



Capital is used to hide IP but users are at risk of being exposed to IP because of VPN software

These are 3 vulnerabilities on HotSpot Shield and have been patched.

1. **Hijack traffic** (CVE-2018-7879) is part of the HotSpot Shield Chrome extension, allowing intrusion and redirection of web traffic to the infected site.
2. **Leak DNS** (CVE-2018-7878) leaks IP users to DNS servers, allowing ISPs to monitor and record activity.
3. **True IP address** leak (CVE-2018-7880) allows hackers to track user locations. This error is due to the whitelist to allow a very loose direct connection. Any domain with localhost such as localhost.foo.bar.com for example, and type = a1fproxyspeedtest in the address bar can bypass proxy and leak real IP.

Note that the above holes are on the Chrome browser utility, not on the mobile application or the software installed on the device.

See more:

1. Russia banned proxy services and VPN to block extreme content
2. China banned VPN services to build the Great Wall
3. The best way to fake IP computer, best

You finished reading the article "**Using HotSpot Shield for security or Facebook access? Your IP is at risk of being exposed**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.