iOS 13.4 release compromises VPN protection

30 March 2020, by Peter Grad

Credit: CC0 Public Domain

Virtual Private Networks are being compromised by a bug in the latest Apple iOS version, 13.4, released last week, according to the online privacy organization ProtonVPN.

The flaw blocks VPN networks from encrypting data in ongoing sessions, allowing information such as IP address and location to be revealed. iPhone users can be exposed to cyberattack if their data is harvested by intruders.

Connections made after the user connects to a VPN are unaffected by the flaw, but connections made prior to VPN activation are not terminated and thus permit the ongoing transmission of unencrypted data.

"Most connections are short-lived and will eventually be re-established through the VPN tunnel on their own," ProtonVPN explained. "However, some are long-lasting and can remain open for minutes to hours outside the VPN tunnel."

Apple's push notifications are cited as an example of connections that remain open and exposed to possible interception.

Due to the nature of iOS security measures surrounding connectivity, a workaround is impossible. According to ProtonVPN, "iOS does not permit a VPN app to kill existing network connections."

Apple says it is examining the issue.

ProtonVPN noted that it first detected the problem with iOS release 13.1.1 in January, but that two months later, with the release of iOS 13.4, no fix has been posted by Apple.

Instead, Apple recommends selecting "Always-on VPN" in Settings, but this offers only limited protection because it does not extend to third-party VPN apps.

ProtonVPN recommended the following steps be taken until a solution is found:

1. Connect to a VPN server.
2. Turn on airplane mode. This will kill all Internet connections and temporarily disconnect the VPN.
3. Turn off airplane mode. The VPN will reconnect, and your other connections should also reconnect inside the VPN tunnel.

ProtonVPN cautioned noted that this alternative, while helpful in many circumstances, is not guaranteed to work in all situations.

VPNs are increasingly popular among consumers working on phones and laptops in public areas such as coffee shops and airports. Privacy networks block others sharing public networks from intercepting a user's connection.

VPNs work by "spoofing," or masking, IP addresses, tricking laptops or mobile devices into thinking they reside in a different location. This helps ensure anonymity and makes identification

difficult, if not impossible. It provides a shield against advertisers who might snoop on your web browsing habits or data thieves lurking on shared networks.

According to a recent report by PC Magazine, "VPNs are necessary for improving individual privacy, but there are also people for whom a VPN is essential for personal and professional safety. Some journalists and political activists rely on VPN services to circumvent government censorship and safely communicate with the outside world."

ProtonVPN observed: "Those at highest risk because of this security flaw are people in countries where surveillance and civil rights abuses are common."

More information:
protonvpn.com/blog/apple-ios-v … rability-disclosure/

APA citation: iOS 13.4 release compromises VPN protection (2020, March 30) retrieved 24 February 2021 from https://techxplore.com/news/2020-03-ios-compromises-vpn.html