Update Teamviewer now if you don't want to be hacked

Teamviewer has released an emergency patch that allows hackers to take control of the computer when they are in the remote control session.

Teamviewer has released an emergency patch that allows hackers to take control of the computer when they are in the remote control session.

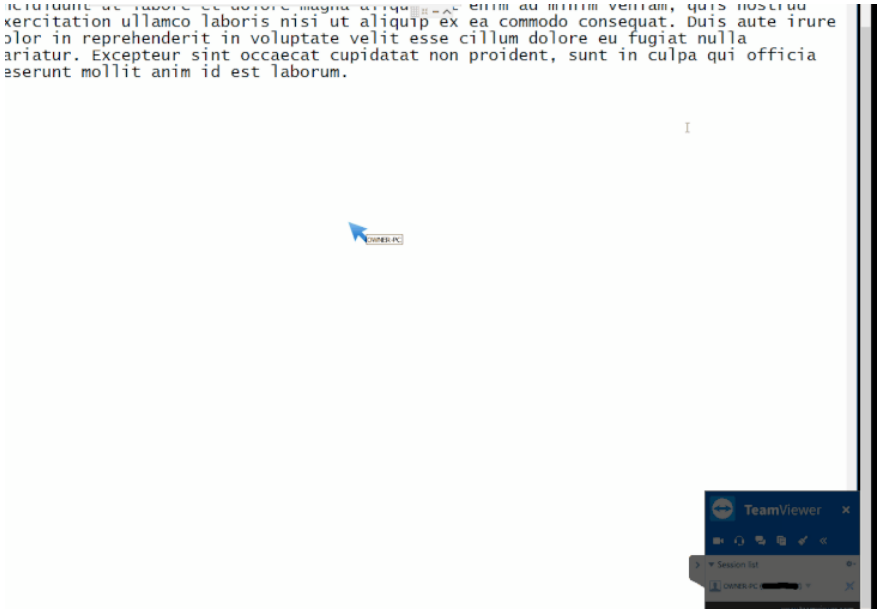
This vulnerability was first discovered on Monday when Reddit users nicknamed 'xployt' said 'be careful'. The user named 'gellin' has downloaded a code of PoC (a C ++ DLL file) to GitHub, tested on TeamViewer version 13.0.5058 to prove the 'location swap' between the two participants of the machine control session count.

See also: What is a DLL file, and how does this file work?

Both server and client side can use this file. If the server side exploits, the hacker will 'fire' the 'location swap' feature and will only be effective when the remote machine authentication has been completed with the client.

Download the latest TeamViewer version at: https://www.teamviewer.com/en/

If the client side exploits, the hacker (from the client side) will take control of the mouse and keyboard without the permission of the server.



Whether a server or client can exploit this vulnerability

Basically to exploit this vulnerability, both parties must authenticate the connection with each other. 'When the code has been injected into the process, it will change the memory value in the process, turn on the GUI elements to change the control. At that time, there is no need for the server to agree that you can access and control the machine, 'gellin said.

TeamViewer has released a patch for Windows, a patch for Linux and macOS will soon be released. Accordingly you need to enable the auto-update feature for TeamViewer to patch the vulnerability.

See also: Instructions for controlling remote computers with TeamViewer