Detecting security on TeamViewer allows hackers to steal the system password remotely

If you are using TeamViewer, you should update to the latest version to avoid security risks.

Recently, the TeamViewer remote control / connection software development team released an unscheduled update to patch a serious security vulnerability. If exploited, this vulnerability, codenamed CVE 2020-13699, allows hackers to remotely steal your computer's system password and then infiltrate it to perform malicious actions.

More worryingly, this attack can be performed almost automatically, without much need for victim interaction. Hackers only need to trick their victim into clicking on a link containing the malicious code once to complete the attack.

Picture 1 of Detecting security on TeamViewer allows hackers to steal the system password remotely

Users should promptly update TeamViewer to the latest version to avoid security risks
TeamViewer is the most popular remote computer connection / control software in the world today. It allows the user to control someone else's computer or vice versa over the Internet, regardless of physical distance.

The CVE 2020-13699 vulnerability was discovered by researcher Jeffrey Hofmann. According to TeamViewer, the problem lies in how they cite their custom URL handlers, allowing hackers to redirect NTLM authentication requests to their systems.

In a nutshell, a hacker can use TeamViewer's URL scheme from a website to trick applications on the victim's system into establishing a connection to their remote SMB shareware. This process triggers an SMB authentication attack, which leaks the system's credentials to help hackers take control of the system or steal victim's data.

To exploit CVE 2020-13699, hacker will have to embed an iframe containing malicious code in a website and then trick the victim into accessing the URL of that website. After the victim clicks the URL, TeamViewer will automatically launch the malicious application on the victim's Windows computer and open the remote SMB share.

Next, the victim's Windows operating system will perform NTLM authentication when opening the SMB share and that request can be forwarded to execute the data, password stealing code.

To avoid being affected, TeamViewer recommends that users upgrade immediately to version 15.8.3. Previously, both Google Chrome, Zoom and Signal had been under an SMB authentication attack.

following us regularly.