TeamViewer Windows Desktop Application Vulnerability and Exploitation

Eranda H.P.D
Cyber Security, Department of Computer Systems Engineering
Faculty of Computing
Sri Lanka Institute of Information Technology
Sri Lanka
dilshan0627@gmail.com

***Abstract*—In the modern world with the massive improvement in technology, now it has become possible to communicate with each other remotely. With the prevailing Covid-19 global pandemic situation, the whole world has moved towards a remote communication era. As a result of this already, most of the people have adapted to the remote desktop technology. This technology is widely used within various private companies & organizations specially by Support Teams & Administrators. This particular technology allows users to easily access to and interact with another computers remotely. Remote Desktop Technology provides the facility to access & use distant computers anytime by staying anywhere.**

The following are some of the fundamental features within Remote Desktop Software.

- **Remote Access & Control**
- **Cross-Platform Support**
- **Multi-Monitor Support**
- **Data Encryption**
- **File Sharing**
- **Mobile Device Access**
- **Session Transferring & Session Recording**
- **Chat**
- **Security & Cloud-based versions**

When it comes to the Remote Desktop Software, there are considerable amount of advantages in it. Efficiency, cost Saving & flexibility are some of the major advantages in this particular Remote Desktop Technology. Following are some of the most commonly used remote desktop software out there in the world. ***(Fig. 1.)***

- **TeamViewer**
- **ConnectWise Control**
- **Splashtop Business Access**
- **AnyDesk**
- **Zoho Assist**
- **VNC Connect**
- **Windows Remote Desktop**
- **Apple Remote Desktop**

However, in this research paper the main focus is set on "TeamViewer Windows Desktop Application".

For the ease of understating, this topic has been divided into several sub-sections.

- **Introduction to TeamViewer Windows Desktop Application**
- **What is CVE-2020-13699**
- **How it occur**
- **Demonstration of the exploitation**
- **What are the bad effects**
- **Affected Versions**
- **Countermeasures**

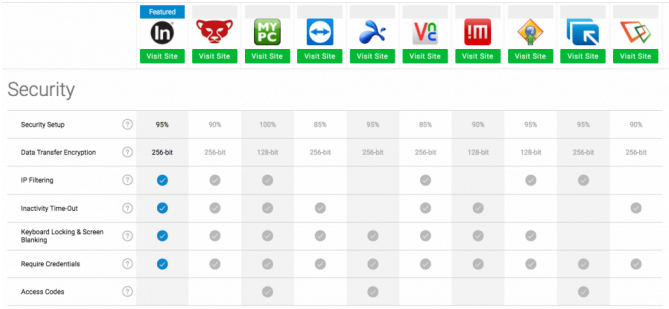

Fig. 1. Security in Remote Desktop Software

***Index Terms*—Common Vulnerabilities and Exposures (CVE), TeamViewer, Risk Analysis, Exploitation, Remote Access, Suspect(client), Victim(host) Threat, Countermeasures**

I. Introduction

TeamViewer is a very fast and a secure all-in-one solution which is generally used to gain access to computers & networks remotely. Additionally, this also supports desktop sharing & file sharing between multiple computers. TeamViewer is a cross-platform or else a platform-independent software which is compatible with multiple operating systems such as Windows, macOS X, Linux, iOS, and Android.

This particular remote desktop software was found in Uhingen, Germany in 2005. It mainly focused on cloud-based technologies in order to establish online remote support and collaboration worldwide. So with the time, TeamViewer Desktop Application evolved massively as the pioneer of innovative remote desktop technology.

According to the TeamViewer's official website [9], currently this software has been installed on over 2.5 billion devices across the whole globe. According to the statistics, there are 45 million devices online at a any given particular time. Due to the COVID-19 pandemic situation all around the world, the enterprise usage of this software has risen up massively as employees were being forced to work from home. TeamViewer also can be used either for commercial use or for private use. Either way, this software consists with a very easy installation process.

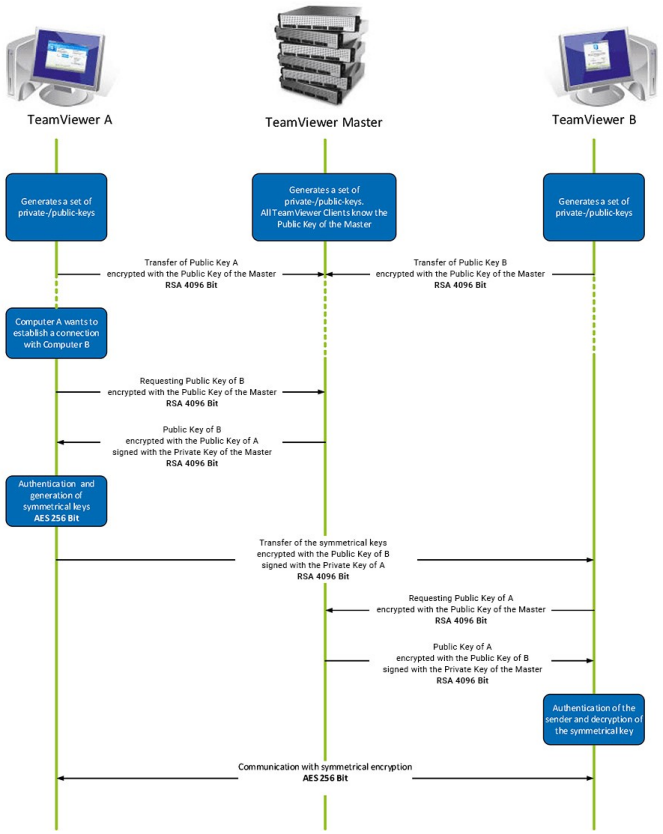

Fig. 2. TeamViewer encryption and authentication

When a particular session is being created, TeamViewer always go for the optimal type of connection. After the handshake procedure with the master server, a direct connection is established via UDP or TCP *(Behind standard gateways, NATs and firewalls)*. As rest of the connections are routed through a **highly redundant router network** *(Using TCP or http-tunnelling)*, there is no need to open any other ports.

When it comes to the security aspect, in order to provide a much more secure connection, this particular software uses **RSA key exchange and AES *(256-bit)*** session encoding mechanism. Since the private key doesn't leave the client PC, it is guaranteed that the data stream between two interconnected computers cannot be deciphered. *(Fig. 2.)* The PKI *(Public Key Infrastructure)* in this encryption mechanism greatly contributes in preventing **"Man-in-the-Middle attacks"**. However, the encryption password exchanging process is never done in a direct manner. When a password verification process is done through a **Challenge-Response Procedure**.*(Fig. 3.)*

Additionally, TeamViewer also uses uses industry-grade security features such as **Two-Factor Authentication** to reinforce the security. In order to comply with **GDPR**, this software has been certified according to **SOC2, HIPAA/HITECH, ISO/IEC 27001, and ISO 9001:2015** standards.

So, now let's move on to the vulnerability.

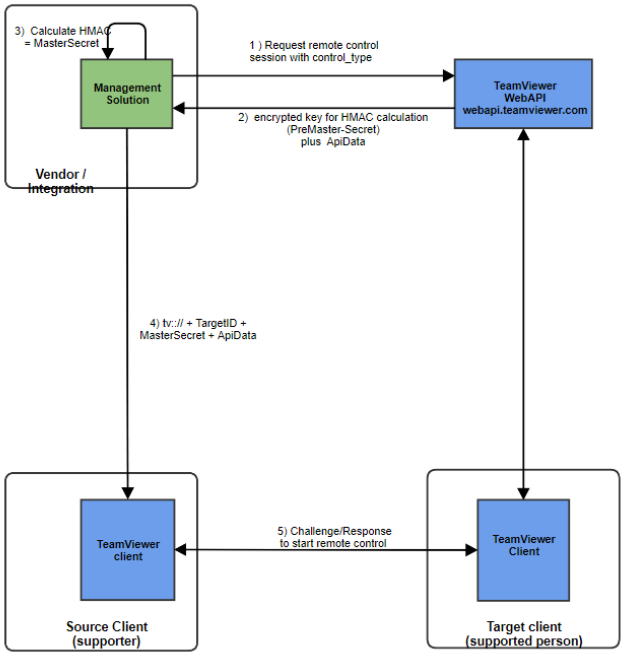

Fig. 3. Challenge-Response Procedure

- What is CVE-2020-13699?
  CVE-2020-13699 is a security weakness which occurs due to an unquoted search path or element. In here, basically the **application does not properly quote its custom URI handlers**. If a system consists with a vulnerable version of TeamViewer installed, when an user visits a malicious website, the vulnerability is going to be exploited.

- How critical is it?
  CVE-2020-13699 vulnerability is categorized as a **High-Risk** Vulnerability in TeamViewer for Windows.(TABLE 1)

	CVSS v3	CVSS v2
Base Score	8.8	6.8
Impact Score	5.9	6.4
Exploitability Score	2.8	8.6

TABLE I
NATIONAL VULNERABILITY DATABASE (NVD)

- How does it impact?
  This particular vulnerability **allows an attacker to capture authentication login credentials and send it to another server**. So, by using the previously authenticated user's privilege, the attacker get the opportunity to perform various malicious operations on the remote server. If an attacker succeeds in exploiting the vulnerability, then it leads the pathway to the attacker to **launch TeamViewer application with arbitrary parameters remotely**. So,

this is going to result in **offline rainbow table attacks** & **brute force cracking attempts.** Additionally, if an attacker was able to successfully exploit this vulnerability, he is going to **obtain sensitive credential information** or in the worst-case scenario, he is going to **take full control over the affected system**.

- What are the affected versions?
  Versions prior to;
  - 8.0.258861
  - 9.0.258860
  - 10.0.258873
  - 11.0.258870
  - 12.0.258869
  - 13.2.36220
  - 14.2.56676
  - 14.7.48350
  - 15.8.3

- What is the solution?
  To address this particular vulnerability, TeamViewer has officially released an update **(High-risk patch)** for their windows desktop application. So all the users of TeamViewer are asked to **upgrade their desktop client** as soon as possible in order to avoid from those malicious attacks.

II. Review of Literature

TeamViewer is a very easy-to-use powerful tool, which is used for remote administration. Because of its massive popularity, this particular software has already become a major target for hackers and for other various threat agents.

As Stjepan Groš says in "Security Risk Assessment of TeamViewer Application" [1], security risk assessment should begin with the identification of all the components that are involved in the application.
When it comes to the TeamViewer desktop application, there are several security controls that needs to be heavily concerned about.

- Logging
- Authentication
- Network protocol & encryption

A. Most common and frequent attack types

In the modern world, there are attackers with different skills & motivations. Sometimes there are massive amount of resources & employees working under those attackers. Attackers try to exploit the application in many different ways. There are some scenarios where the attacks do not impact applications directly, but via some other means.

When it comes to the attack types, mainly there are two types of attacks which are inside attacks & outside attacks. Among those, inside attacks are more severe than the outside attacks. Inside attacks are much more difficult to detect because the users are authenticated in that particular domain already.

According to "TeamViewer Security Statement" [2], in TeamViewer application, the IDs are generated based on the hardware characteristics. The application servers are capable of checking the validity of IDs before a connection is established.

B. Defense mechanism of TeamViewer

When it comes to the application security of the TeamViewer desktop application, there are several important security mechanisms implemented within it.

- **Blacklist & Whitelist**
  - When maintaining unattended computers *(As a Windows service)*, the access can be limited only for specific number of clients.
  - Blacklist & Whitelist functions enable the ability to explicitly block or allow certain TeamViewer IDs.

- **No Stealth Mode**
  - TeamViewer desktop application does not allow to run itself in the background without properly notifying the user.
  - Even after the connection is established, a small control panel icon is popped within the system toolbars.

- **Password Protection**
  - When it comes to the password protection, generally TeamViewer uses a one-time session password for a particular client.
  - Whenever a client's computer gets rebooted, a new session password is generated for that computer.
  - However, individual fixed passwords are used in special case scenarios such as when deploying TeamViewer desktop application for unattended remote support *(servers)*.

- **Access Controlling in Incoming & Outgoing Traffic**
  - Connection modes can be individually configured within this application.
  - A particular client computer can be configured to deny only the incoming connections.
  - This helps greatly in reducing the potential threats & vulnerabilities.

C. How the vulnerability occur?

According to the security blog-post made by Silviu Stahie in [3], bad actors who could set up a phishing site including a malicious iframe can launch the TeamViewer client soon after victim opened the website.TeamViewer Windows Desktop client versions that were released prior 15.8.3, were unable to properly quote its custom URI handlers. So there is a huge possibility of getting this vulnerability easily exploited.

D. How the attack is performed?

According to a security forum written by Martin Beltov in [4], it has been identified that CVE-2020-13699 is a very dangerous & a critical security vulnerability. The hackers take the full advantage of un-patched versions the TeamViewer Desktop Application by generating specially-crafted malicious sites. So when an user clicks on either of those links, he is automatically forced to run and open a SAMBA share. Basically, SAMBA Share is a network sharing feature which is included in the operating system that allows the data to be available over the network. So due to the programming code fault, the authenticated network share allows an attacker to perform **Remote Code Execution**.

Usually it's the responsibility of the apps, to identify & properly handle the URI's for the websites. But, as handler applications are capable of receiving data from untrusted sources, the URI values which are passed towards the application might contain malicious data that have the potential of exploiting the app. Basically, TeamViewer treats those as "commands" rather than as "input values". As Lindsey O'Donnell says in her blog-post [5], it is possible to easily exploit this particular vulnerability by unauthenticated, remote attackers in order to execute code & crack passwords of victims. To initiate the attack, the only thing that an attacker needs to perform is persuading a victim to click on crafted URL in a particular website. So this creates a potential window for the attacker to create watering-hole attacks. When a particular victim's TeamViewer desktop client application begins the remote SMB share, then Windows is going to establish the connection using **New Technology LAN Manager *(NTLM)***. Usually this NTLM uses an encrypted protocol specially when authenticating an user without providing user's password. Basically, those NTLM credentials are purely based on previously acquired data samples that are collected during interactive logon process. Additionally, those logon credentials consist with a username, a domain name and a one-way hash of the user's password.

According to Jeffrey Hofmann [6], attackers use the NTLM request for relayed attacks as well. In order to perform such kind of attacks, an attacker uses special tools such as Responder. This particular tool is capable of capturing SMB authentication sessions on an internal network. Then, those sessions are used to relay to a target machine. So obviously this lead the pathway to the attackers to access of the victim's machine.

E. Impact of the attack & solutions

According to Lindsey O'Donnell in [5], when it comes to the impact level, **there is a massive gap between the expected impact level & the practical impact level.** But for a successful exploitation, there is a huge set of prerequisites out there that needs to be full filled first. However, TeamViewer has stated that they have implemented some major improvements & security patches specially in URI handling relating to CVE 2020-13699.

```
622  <section class="bc_main_content">
623  <div class="container">
624  <div class="row">
625  <div class="col-md-8">
626  <div class="cz-main-left-section">
627  <div class="bc_latest_news">
628      <iframe style="height:1px;width:1px;" src="teamviewer10: --play
     \\attacker-IP\share\fake.tvs"></iframe>
629  <div class="cz-line-heading lheader"><div class="cz-line-heading-inner"
     >Latest Articles</div></div>
630  <ul id="bc-home-news-main-wrap"><li>
631  <div class="bc_latest_news_img">
632  <a href="https://www.bleepingcomputer.com/news/microsoft/
     chromium-browser-sneaked-through-review-released-on-microsoft-store/">
```

Fig. 4. Setting iframe's src attribute

III. Methodology

The high-severity bug in TeamViewer Remote Desktop Application, "CVE-2020-13699", can be categorized as **dubbed Unquoted Search Path or Element *(CWE-428)***. Basicaly in here, the arguments that are being passed to a particular program are **not quoted.** So this may result in **"treating the arguments as direct commands, rather than an input value".**

But in order to perform a successful attack, a victim user needs to click on a malicious website or a link. Then that particular page loads an iframe in victim's web browser in a perfectly hidden manner. So that the victim is unable to identify the background attacking process. The iframe is capable of loading itself by using the **"teamviewer10:"** URI scheme. So this demands the victim's web browser to launch the TeamViewer Desktop Application on his computer. Usually, custom URI schemes are mostly used by the locally installed applications. So, this encourages the victim users to launch it from their web browsers.

As you can see in the above Fig. 1, in order to exploit this particular vulnerability an attacker are required to set iframe's src attribute to **"teamviewer10: –play \\attacker-IP\share\fake.tvs"**. This particular command tells the TeamViewer client application to connect to the attacker's server via the Server Message Block (SMB) protocol. So, when this command is used, first it launches the TeamViewer desktop client & after that it's going to force open a remote SMB share.

In here, the attacker does not actually need to know the victim's password because the connection is initiated from victim's machine to attacker's SMB share. So as a result of that, the attacker is going to be authenticated automatically.

According to Hofmann [4], multiple versions of TeamViewer were impacted from the URI schemes that could be used in the attack.

- The following URI handlers were affected by this.
  - teamviewer10/8
  - tvpresent1
  - teamviewerapi
  - tvcontrol1
  - tvfiletransfer1
  - tvsqcustomer1
  - tvsqsupport1
  - tvvideocall1
  - tvvpn1

Fig. 5. Information about the Vulnerability

Fig. 6. Set options

IV. Results

In order to practically demonstrate this exploitation, a Kali Linux virtual machine & a Windows virtual machine are required. Kali Linux OS is already packed with massive amount of penetration testing tools. Among those, in order to perform this exploitation **"Metasploit Framework"** & **"Responder"** tools are required.

First of all it's necessary to identify the particular vulnerability properly using the Metasploit Framework. After correctly choosing the vulnerability, it is possible to view a comprehensive description about that particular vulnerability. *(Fig. 5.)*

After that, it is mandatory to set the options for both **"SMB SERVER"** & **"SRVHOST"**. *(Fig. 6.)* Then it is required to use the Responder tool, in order to gain remote system access to the Windows virtual machine. *(Fig. 7.)* When the "run" command is given, it automatically generates a malicious link and send towards the Windows virtual machine. *(Fig. 8.)* If the exploitation is performed successfully, victim machine's hashed password can be captured easily by an attacker. *(Fig. 9.)*

V. Conclusion

In this extensive research paper, almost all the areas are covered regarding the TeamViewer Desktop Application vulnerability and exploitation. With the prevailing Covid-19 pandemic situation, most of the people have moved towards the remote communication technologies. Currently, Remote Desktop Technology is mostly being used specially in technical support

Fig. 7. Gaining Remote System Access using Responder tool

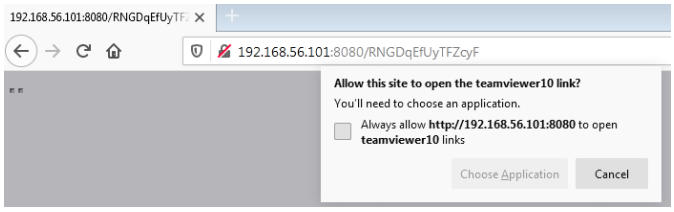

Fig. 8. Receiving the malicious link

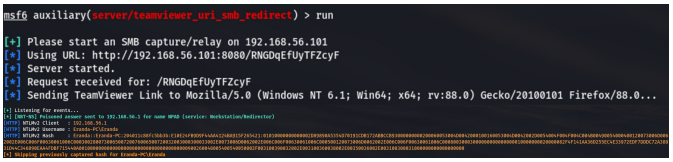

Fig. 9. Hashed Password of victim's machine

industry. When it comes to the remote desktop software, there are massive number of features & advantages in it. Although there are huge variety of remote desktop software out there, TeamViewer is the most popular & commonly used remote desktop software among those.

TeamViewer can be considered as a very fast & secure all-in-one solution which is used to access other computers remotely. When the security aspect of TeamViewer is concerned, in the session encoding process, this software uses RSA key exchange and AES *(256-bit)*. This contributes a lot specially in establishing a secure connection. As a result of that, it is guaranteed that the data stream between two interconnected computers cannot be deciphered. In order to gain more trust towards the software, TeamViewer uses additional security features also such as Two-Factor Authentication. Furthermore TeamViewer has been able to adapt according to global standards such as SOC2, HIPAA/HITECH, ISO/IEC 27001, and ISO 9001:2015.

CVE-2020-13699 is considered as a major security flow within the TeamViewer desktop application. Usually this vulnerability occur due to an unquoted search path or element. The main reason for this issue is that the application does not properly quote its custom URI handlers. If a particular computer is installed with a vulnerable version of TeamViewer, then the previously mentioned vulnerability is going to be exploited soon after when an user visits a malicious website.

This high-risk vulnerability is capable of generating a massive impact on the victim. It allows an attacker to steal authentication login credentials of a particular user and send it to another remote server. After an attacker successfully gains access over a system, he gets the opportunity to perform various malicious operations on the remote server. As a result of this eventually the attacker gets the authorization to launch TeamViewer application with arbitrary parameters remotely. This leads the pathway to the attacker to perform offline rainbow table attacks & brute force cracking attempts on the target machine.

Almost all the TeamViewer versions released before the version 15.8.3, are affected by this particular vulnerability. In order to solve this security issue, TeamViewer has officially released a High-Risk patch for their windows desktop application. The company itself has advised its all the users to upgrade their desktop client application to the latest version as soon as possible.

ACKNOWLEDGEMENT

As the 3rd year 1st semester Cyber Security undergraduates at SLIIT, under the module Secure Software Systems (IE3042), we were asked to write a research paper on a web or software security related topic. After done writing the research paper, we are supposed to create a video explaining the demonstration process of that chosen topic.The Software Security related topic that I have chosen is "TeamViewer Windows Desktop Application Vulnerability and Exploitation".

First of all, I would be very grateful to our lecturer in charge Dr. Lakmal Rupasinghe for giving me this wonderful opportunity to enhance my knowledge and experience on software security. His immense kind and consistent support helped me a lot specially in choosing a better topic for this assignment. Not only that, he also checks our assignment progress weekly by randomly selecting students during the webinar sessions. This has provided us with a valuable opportunity to correct our mistakes weekly in our assignment.

So once again I would like to express my greatest gratitude to the Lecturer in Charge and associated lecturers for guiding me throughout this entire research project.

REFERENCES

[1] Groš, S. (2011, June). Security risk assessment of TeamViewer application. In Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces (pp. 103-108). IEEE.

[2] Yumpu.com. "Teamviewer Security Statement". Yumpu.Com, https://www.yumpu.com/en/document/read/348593/teamviewer-security-statement. Accessed 30 May 2021.

[3] STAHIE, Silviu. "Severe TeamViewer Vulnerability Let Attackers Steal System Password." HotForSecurity, Sept. 2020, https://hotforsecurity.bitdefender.com/blog/severe-teamviewer-vulnerability-let-attackers-steal-system-password-23926.html.

[4] Beltov, Martin. "CVE-2020-13699: Critical TeamViewer Flaw Allows Hackers To Exploit User Devices". SENSORSTechForum, 7 Aug. 2020, https://sensorstechforum.com/cve-2020-13699-teamviewer/.

[5] O'Donnell, Lindsey. "TeamViewer Flaw in Windows App Allows Password-Cracking". Aug. 2020, https://threatpost.com/teamviewer-fhigh-severity-flaw-windows-app/158204/.

[6] Jeffrey Hofmann, "security engineer at Praetorian", The person who disclosed this flaw.

[7] Paganini, Pierluigi. "TeamViewer Flaw Can Allow Hackers to Steal System Password". SecurityAffairs, 11 Aug. 2020, https://securityaffairs.co/wordpress/106978/breaking-news/teamviewer-flaw-system-password.html.

[8] Sharma, Ax. "TeamViewer Fixes Bug That Lets Attackers Access Your PC". BleepingComputer, 7 Aug. 2020, https://www.bleepingcomputer.com/news/security/teamviewer-fixes-bug-that-lets-attackers-access-your-pc/.

[9] "TeamViewer: The Remote Desktop Software, TeamViewer", https://www.teamviewer.com/en-us/. Accessed 7 June 2021.