

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<https://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

08/05/2020

**SUBJECT:**

A Vulnerability in TeamViewer Could Allow for Offline Password Cracking

**OVERVIEW:**

A vulnerability has been discovered in TeamViewer, which could allow for offline password cracking. TeamViewer is a program used for remote control, desktop sharing, online meetings, web conferencing, and file transfer between systems. Successful exploitation of this vulnerability could allow an attacker to launch TeamViewer with arbitrary parameters. The program could be forced to relay an NTLM authentication request to the attacker's system allowing 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.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- TeamViewer versions 15.8.3 and prior

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

A vulnerability has been discovered in TeamViewer, which could allow for offline password cracking. Specifically, this vulnerability is due to the program not properly quoting its custom URI handlers. This vulnerability can be exploited when the system visits a maliciously crafted website.

Successful exploitation of this vulnerability could allow an attacker to launch TeamViewer with arbitrary parameters. The program could be forced to relay an NTLM authentication request to the attacker's system allowing 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.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches from TeamViewer to the vulnerable systems after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources.

#### **REFERENCES:**

##### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13699>

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<https://www.us-cert.gov/tlp/>