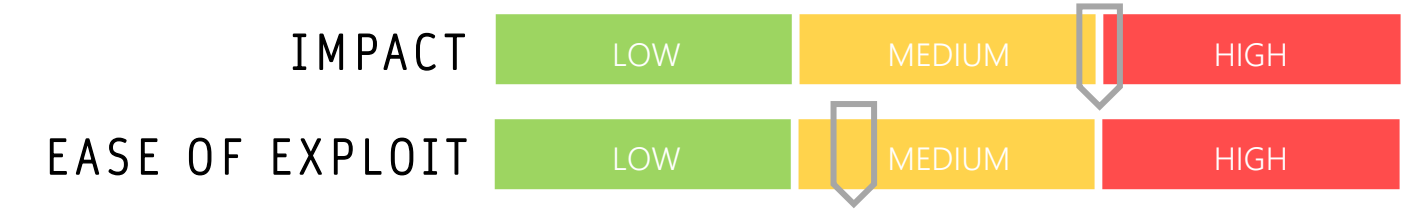
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00020

TEAMVIEWER FLAW IN WINDOWS

DATE ISSUED: 10th August 2020



OVERVIEW

Popular remote access and support software TeamViewer has had a flaw discovered recently that allows remote, unauthenticated access for password cracking and remote code execution in Windows systems.

BREAKDOWN

The Windows desktop application suffers from not quoting custom Uniform Resource Identifiers (URIs) properly, allowing untrusted sources to pass malicious data to the application through iframes injected into a website, forcing it to open an SMB share. After which a connection is initiated through NT LAN Manager and may be relayed by an attacker using a tool such as Responder, granting access to the machine for the attacker, allowing the capture of password hashes. These may be cracked thereafter by brute force, thereafter, leading to further system compromise.

CVE 2020-13699

REMEDIATION STEPS

- Update to the latest version of TeamViewer to ensure your version contains the latest improvements to the URI handling process v15.8.3
- Investigate alternate remote access service software that may be more suitable for your organization
- Educate users surrounding risks posed by untrusted sources and email links or attachments
- Ensure sufficient URL filtering is in place to prevent connection to untrusted sources

REFERENCES & RESOURCES

Security Affairs: https://securityaffairs.co/wordpress/106978/breaking-news/teamviewer-flaw-system-password.html
The Hacker News: https://thehackernews.com/2020/08/teamviewer-password-hacking.html
Threatpost: https://threatpost.com/teamviewer-fhigh-severity-flaw-windows-app/158204/