Report CVE 2020 Windows 10

* Mô tả Vul
* Cách phát hiện
* Exploit như nào

CVE-2020-13699

Mô tả: TeamViewer Desktop for Windows before 15.8.3 does not properly quote its custom URI handlers. A malicious website could launch TeamViewer with arbitrary parameters, as demonstrated by a teamviewer10: --play URL. An attacker could force a victim to send an NTLM authentication request and either relay the request or capture the hash for offline password cracking. This affects teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1, and tvvpn1. The issue is fixed in 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350, and 15.8.3.

This module exploits an unquoted parameter call within the Teamviewer URI handler to create an SMB connection to an attacker controlled IP. TeamViewer < 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350, and 15.8.3 are vulnerable. Only Firefox can be exploited by this vulnerability, as all other browsers encode the space after 'play' and before the SMB location, preventing successful exploitation. Teamviewer 15.4.4445, and 8.0.16642 were succssfully tested against.

Cách phát hiện: update lên phiên bản mới nhất

Exploit như nào: [TeamViewer Vulnerability (CVE-2020-13699) Metasploit - YouTube](https://www.youtube.com/watch?v=AmMa40XS14Y)