Zoom has another security flaw

2 April 2020, by Bob Yirka

Credit: CC0 Public Domain

Researchers at a company called Bleeping Computer have exposed another security flaw with the conferencing application Zoom—one that allows hackers to steal user passwords. The vulnerability in the software application comes at a time when its popularity has skyrocketed as employees use it to work from home due to the ongoing global pandemic.

Zoom is a web-based application that allows multiple people to log into an online conference. Once logged in, those in the meeting can see and hear one another and also send documents and graphics back and forth—just as they might in a face-to-face meeting. Unfortunately, the application has been beset with security issues, including hackers breaking into meetings to create disruptions. Now, it appears the application has another more serious security problem—it allows hackers to steal Microsoft Windows passwords, which can be used to access programs and data on computers and network servers.

The vulnerability involves users clicking on a link that has been shared in a chat by someone who has joined a meeting. Clicking on it sends the user's credentials to the person who sent the link—that person can then use information in the credentials to access the user's computer—security researcher Matthew Hickey has announced on his Twitter feed that the hack can also be used to launch programs installed on a victim's computer. More specifically, when a user clicks on the link, Windows makes an attempt to connect to a remote site using the SMB file sharing protocol and open a file specified in the link. Such an attack is known as a UNC path injection, and it works for hackers because Windows does not hide a user's login name and password when they attempt to access a remote server. The password is encrypted, but as several Twitter users have pointed out, it can be easily cracked using available third-party tools.

Engineers at Zoom are reportedly working on a fix for the vulnerability, even as officials with the company have noted that users can close the vulnerability by making changes to their Windows settings—by turning off automatic transmission of NTML credentials to a remote server.

APA citation: Zoom has another security flaw (2020, April 2) retrieved 2 December 2020 from https://techxplore.com/news/2020-04-flaw.html