Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

April 9, 2020
CS-04-2020

Collaboration Application Security

OVERVIEW

With the rapid increase of work-from-home or teleworking in the state of Michigan, there has been a surge in the usage of collaboration applications. Whether it's sending messages, setting up virtual calls, or coordinating virtual meetings, online collaboration applications have become a required tool for keeping organizations operational. Some of the more popular applications include Microsoft Teams, Skype, Zoom, Slack, Ryver, Discord, Facebook Messenger, GoToMeeting, Google Hangouts, Cisco Webex, Adobe Connect, etc.

Malicious cyber actors are currently targeting collaboration platforms, as well as other online communication tools, to eavesdrop on conference calls or overload services and subsequently take them offline. Cyber actors have also reportedly hijacked or "zoom-bombed" teleconferences by utilizing the video streaming, screen sharing, and chat features to share unsolicited pornographic images, hate images, or threatening/crude remarks. Researchers have also discovered malware, such as cyrptocurrency-mining software, embedded in the installation package for certain collaboration applications. The Michigan Cyber Command Center (MC3) recommends only downloading applications from their official website, as well as the following operational security control measures.

LIMIT SENSITIVE DATA DISCUSSION

Whether sending messages or utilizing teleconference capabilities, the MC3 recommends not discussing sensitive or confidential topics or display/transfer sensitive data in collaboration applications. Users should understand if the application is storing data, such as messages or recordings of voice or video calls, and how this storage is being handled. Is the data stored locally in the application or on a cloud based server? Is the data stored encrypted or in plain text? Users should be cognizant if the organization shares or sells any of the information with third parties. The best practice in avoiding this risk is not discussing sensitive information on these platforms.

CONTROL ACCESS

1. Use a Unique ID when setting up meetings.
2. Utilize invite-only meetings whenever possible.
3. Require a meeting password that can not be easily guessed.
    - Do not use a date or common pin for a password.
4. Create and utilize waiting rooms.
5. Lock meetings once they have started.

MEETING MANAGEMENT

1. Limit screen sharing or host sharing.
2. Limit or disable cameras and microphones when necessary.
    - If possible, disable microphones and cameras at the start and then enable access if necessary.
3. Remove or block guests when necessary and enable settings that do not permit them to return, if removed.
4. Remove or prevent animated GIFs and other files in the chat or disable the chat altogether if there is a concern for inappropriate comments.
5. Disable private chat to limit the opportunity an unwanted guest has to harass others on the call.

RESOURCES

https://www.ic3.gov/media/2020/200401.aspx
Any additional questions or concerns can be sent to mc3@michigan.gov or 1-877-MI-CYBER.