NORTH Dakota Be Legendary.™ | Joint Information Center INFORMATION TECHNOLOGY

Zoom Meetings Virtual Conferencing Platform Assessment & Guidelines

Prepared April 8, 2020

In the interest of transparency, and pursuant to its responsibility to "advise and oversee cybersecurity strategy for all executive branch state agencies, including institutions under the control of the state board of higher education, counties, cities, school districts, or other political subdivisions," the North Dakota Information Technology (NDIT) Cyber Operations Center (CyOC) is sharing the results of its risk assessment of the Zoom Meetings virtual conferencing platform. It is the CyOC's intent to help State Government, private organizations and citizens evaluate the risk to their security and privacy and to inform them of best practices to mitigate risks associated with Zoom Meetings and web conferencing in general.

Threat Statements:

The CyOC observes that Cyber criminals and hackers are targeting users of virtual conferencing platforms (e.g., Zoom Meetings, Teams, Google Classroom, and Cisco WebX), and that the growing popularity of this technology leaves users open to attacks that may disrupt work, destroy property, invade privacy, and cause financial harm. The CyOC reviewed vulnerabilities in the National Vulnerability Database as well as active threat intelligence regarding the Zoom Meetings platform and makes the following observations:

1) **Zoom Meetings' encryption may not be adequate to secure sensitive information or protect the privacy of individuals in meetings (CVE-2020-11500 High Risk):**
   - Though Zoom Meetings advertises the use of AES-256-bit encryption, researchers have observed that Zoom uses only an AES-128 key for encryption that is shared by all users in the meeting. This is not as secure as the AES-256-bit encryption of other conferencing software.
   - Researchers have observed that Zoom Meetings uses encryption in the AES Electronic Code Book (ECB) mode which is weaker than the Secure RTP standards for streaming media. ECB mode preserves patterns and may allow malicious actors to see images in videos.

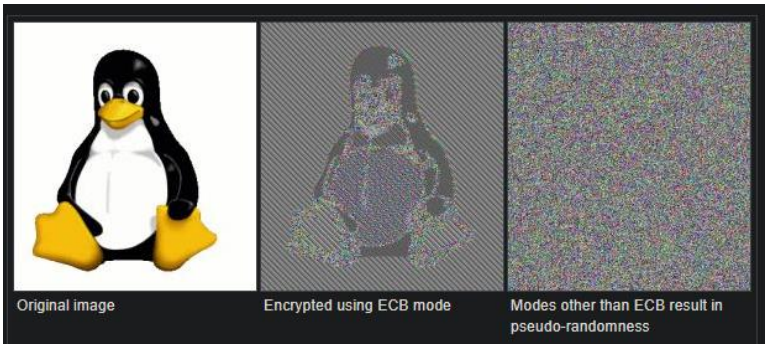

Figure 1: Tux the Penguin Encrypted in ECB vs Pseudo-Random Encryption: Source github picoctf-2019-solutions/Cryptography/aes-abc/readme.md

- Researchers found encryption key distribution servers for U.S.-based Zoom Meetings sessions in Beijing, China. In some cases, Zoom Meetings may be legally obligated to disclose encryption keys for meetings to the Chinese Government.

2) **The Zoom Meetings client may allow local malicious processes to run as root, or to access microphone and camera resources of macOS devices (CVE-2020-11469 High Risk, & CVE-2020-11470 Low Risk):**
   - The Zoom Meetings installer copies 'runwithroot' to a writable temporary directory that allows malicious code to execute by writing to the same directory.
   - The Zoom Meetings installer files are currently being used to distribute malicious files. Once a user downloads the malicious file, additional malicious software can be installed on MacOS devices.
   - Installation of malicious code via this method may also inherit Zoom Meetings' ability to obtain access to microphones and cameras allowing the malicious process to turn cameras and microphones on and off.

3) **Zoom Meetings and other web conferencing applications are vulnerable to multiple attacks:**
   - Malicious actors are creating fake installation files for multiple meeting platforms including Zoom Meetings, MS Teams, and Google Classroom.
   - Zoom Meetings and other conferencing platforms have been "conference bombed," when an uninvited guest gained access to meetings to disrupt the conference and/or eavesdrop on conversations.
   - Zoom Meetings users have been targeted to capture potentially sensitive data disclosed during meetings and/or to access previously recorded meetings not stored in a secure manner. Attackers have accessed Zoom Meetings files stored on a computers and unsecured public cloud environments.

The CyOC notes that **there is no indication that these vulnerabilities are mitigated with a distribution or payed version of Zoom Meetings**.

Risk and Impact Statements:

Through a review and discussion with multiple NDIT team members, the CyOC believes that threats to virtual conferencing users span all branches of State Government. Additionally, most state-level users are impacted as either participants or hosts of Zoom meetings.

Three agencies have been identified as high-volume Zoom users based on the number of users within the entity, or the amount of business they transact using Zoom:

- NDIT – Key vendors use Zoom as the primary method of conducting virtual meetings with NDIT. Potentially sensitive information is discussed during these meeting, utilizing chat, shared screens and voice tools. Typically, NDIT is a Zoom participant, but occasionally hosts Zoom meetings as well.
- K-12 – Zoom has become an alternative video-conferencing tool used by teachers instead of Microsoft Teams to conduct virtual learning sessions for K-12. K-12 also participates in Zoom meetings hosted by vendors and associations.
- DHS – To the Department of Human Services'(DHS) knowledge, DHS is primarily a participant in Zoom meetings hosted by external parties, such as federal partners, and no confidential information is being disclosed using standard versions of Zoom. DHS's legal team is advising program directors to use Teams; however, they still need to be able to participate in Zoom meetings to conduct business. No confidential information shall be disclosed unless the Healthcare for Zoom platform is being utilized or another paid version of Zoom Meetings.

Re-evaluation Period

The CyOC observes that Zoom has issued a public apology for security issues associated with the platform and will be entering a 90-day feature freeze to direct resources toward fixing privacy and security issues. The CyOC will re-evaluate the risk of the Zoom platform after this 90-day period has expired and issue new guidance if warranted.

Recommendations

NDIT offers a variety of services and tools to help state entities through this challenging time. We also recognize there are a variety of situations that may impact which virtual conferencing solution a state entity may choose to use. If you have questions or concerns, please reach out to the NDIT Service Desk at 701.328.4470.

Microsoft Teams:

The CyOC recommends agencies and state employees use Microsoft Teams as their virtual communication platform of choice. NDIT manages a Microsoft environment for the State and has a highly effective capability to secure the environment in which it runs. NDIT's managed Teams application is demonstrated to be a very flexible, stable and effective tool to help organizations securely communicate and collaborate (via phone, instant messaging, file sharing, and custom channels that can offer restricted access). Additionally, as the Microsoft environment is managed by NDIT, users may rely on the authenticity of the files used for installation of the Teams application.

K-12 Alignment with the State's Education Technology Services:

The CyOC further recommends that ND K-12 school districts and educational organizations adopt Microsoft Teams through the ND IT K-12 educational technology division (EduTech) as their virtual communication platform of choice. Those school districts deploying their own managed Microsoft Teams instance should contact EduTech to make sure they are aligned with the state's security posture. Schools using Zoom and other virtual conferencing software must ensure that their selected technology is not deployed in a manner that places educational data at risk or violates applicable data privacy laws. Please be warned that free-to-use solutions generally lack data privacy agreements.

Anti-Malware:

The CyOC observes that the vulnerabilities in Zoom Meetings may provide attackers a deployment method for ransomware and other malware. Many largescale ransomware incidents occurred on systems that are protected by traditional signature-based antimalware. As such, the CyOC recommends that all government organizations adopt the CyOC's implementation of next-generation antimalware. The CyOC's next-generation antimalware solution has been shown to be effective against ransomware and other malware variants that may go undetected by traditional antimalware applications.

Guidelines for Virtual Conferencing:

Below are some helpful recommendations to improve the privacy and security of web based virtual meetings:

1. Do not share sensitive data during non-Teams virtual conference meetings.
2. Become familiar with who may record your meeting. Be aware that individuals may choose to record a meeting using audio or video recording tools outside of the meeting software.
3. Download virtual conferencing clients directly from the manufacturer or your service provider.
4. Always run the newest version of the conferencing client (if required to download and install a client).
5. Password protect each meeting with a unique and complex password using letters, numbers and special characters.
6. Password protect recordings of meetings with a unique and complex password using letters, numbers and special characters.
7. Do not share your meeting link in public forums or on social media. In the event you must advertise your meeting publicly, remove the password embedded in the link and ask attendees to contact the organizer for the password.
8. Use a meeting ID rather than the personal ID associated with a virtual conferencing account. This way the meeting ID should change for each meeting.
9. Disable sharing for all attendees except for the meeting host.

10. Use the waiting room/lobby feature when it is available. This requires the organizers to admit people singly (for small meetings) or all at once (for larger meetings). If an attendee seems suspicious, the waiting room feature allows organizers to prevent them from joining the meeting.
11. Remove and block anyone from meeting rooms with an unrecognizable or unverifiable identity. Once removed, the person or people cannot come back in.

Taking the above steps is good virtual meeting practice and will promote private and secure meetings to collaborate, connect and remain productive.