CySecK ಸಲಹೆ -

ಆನ್‌ಲೈನ್ ಸಭೆಗಳಲ್ಲಿ ಜೂಮ್ (Zoom) ಬಳಕೆ

ಪ್ರಕಟಣೆ: 17-ಏಪ್ರಿಲ್ -2020

ಸಲಹಾ ಸಾರಾಂಶ

ಜೂಮ್ ಆನ್‌ಲೈನ್ ಮೀಟಿಂಗ್ / ವೆಬಿನಾರ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ ಹಲವಾರು ಸುರಕ್ಷತೆ ಮತ್ತು ಗೌಪ್ಯತೆ ಸಮಸ್ಯೆಗಳನ್ನು ಗುರುತಿಸಲಾಗಿದೆ. ಈ ಸಮಸ್ಯೆಗಳನ್ನು ಗಮನದಲ್ಲಿರಿಸಿ ಕೆಳಕಂಡ ಪರಿಹಾರಗಳ ಶಿಫಾರಸು ಮಾಡಲಾಗಿದೆ:

1. ಸರ್ಕಾರಿ ಅಧಿಕಾರಿಗಳು / ಕಚೇರಿಗಳು ಆನ್‌ಲೈನ್ ಸಭೆಗಳಿಗಾಗಿ ಜೂಮ್ ಅನ್ನು ಬಳಸಬಾರದೆಂದು ಸೂಚಿಸಲಾಗಿದೆ.
2. ಖಾಸಗಿ ವ್ಯಕ್ತಿಗಳು / ಉದ್ಯಮಗಳು ತಮ್ಮ ಯಾವುದೇ ಸಭೆಗಳಲ್ಲಿ ಗೌಪ್ಯವಾದ / ಗುಟ್ಟಾದ ವಿಷಯಗಳನ್ನು ಚರ್ಚಿಸುವಾಗ ಜೂಮ್ ಅನ್ನು ಬಳಸದಿದ್ದರೆ ಉತ್ತಮವೆಂದು ಶಿಫಾರಸು ಮಾಡಲಾಗಿದೆ. ನೀವು ಜೂಮ್ ಲೈಸೆನ್ಸುಗಳನ್ನು ಖರೀದಿಸಿದ್ದರೆ, ಗೌಪ್ಯವಲ್ಲದ ಸಭೆಗಳಿಗಾಗಿ ಹೂಡಿದ ಅವಧಿಯನ್ನು ಬಳಸುವುದನ್ನು ನೀವು ಮುಂದುವರೆಸಬಹುದು.
3. ಜೂಮ್ ಬಳಸುವ ಎಲ್ಲ ಖಾಸಗಿ ವ್ಯಕ್ತಿಗಳು / ಉದ್ಯಮಗಳು ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ನಲ್ಲಿ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಮರುಪರಿಶೀಲಿಸಬೇಕು ಮತ್ತು ಅತ್ಯುತ್ತಮ ಅಭ್ಯಾಸಗಳನ್ನು ಅನುಸರಿಸಬೇಕು.
4. ತಮ್ಮ ಸಿಸ್ಟಂಗಳಲ್ಲಿ ಇತ್ತೀಚಿನ ಆವೃತ್ತಿಗೆ ಜೂಮ್ ಕ್ಲೈಂಟನ್ನು ನವೀಕರಿಸಲು ಎಲ್ಲಾ ಬಳಕೆದಾರರಿಗೆ ಸಲಹೆ ನೀಡಬೇಕು.

ಶಿಫಾರಸಾದ ಪ್ರಮುಖ ಸೆಟ್ಟಿಂಗ್‌ಗಳು

ಕೆಳಗೆ ಶಿಫಾರಸಾದ ಪ್ರಮುಖ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಜೂಮ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮಿನಲ್ಲಿ ರೂಪಿಸಿಕೊಳ್ಳಿ.

1. ಭಾಗಿದಾರರಿಗೆ ಲಾಗಿನ್ ಮಾಡಿದ ನಂತರ ಮತ್ತು ಸಭೆಗೆ ಸೇರುವ ಮುನ್ನ ಹೋಸ್ಟ್ (ಗಳು) ಸ್ಪಷ್ಟವಾಗಿ ಪ್ರವೇಶ ನೀಡಬೇಕಾಗುವಂತೆ ಜೂಮ್‌ನ ವೇಟಿಂಗ್ ರೂಮ್ ಫೀಚರ್ ಬಳಸಿ .
2. ಕರೆಗಳು ವೀಡಿಯೊ ಹಾಗು ಆಡಿಯೊ ಡಿಫಾಲ್ಟಾಗಿ ಮ್ಯೂಟ್ ಆಗಿ ಪ್ರಾರಂಭವಾಗುವಂತೆ, ಮತ್ತು ಯಾರು ಮಾತನಾಡಬಹುದು/ ವೀಡಿಯೊ ಹಂಚಿಕೊಳ್ಳಬಹುದೆಂಬುದನ್ನು ಹೋಸ್ಟ್ (ಗಳು) ಮಾತ್ರ ನಿರ್ಧರಿಸುವಂತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ರೂಪಿಸಿ.
3. ಒಳನುಗ್ಗುವವರನ್ನು ಸುಲಭವಾಗಿ ಗುರುತಿಸಲು ಸುಲಭವಾಗಿಸಲು ಗುರುತಿಸಬಹುದಾದ ಹೆಸರಿನೊಂದಿಗೆ ಜೂಮ್ ಅಕೌಂಟಿಗೆ ಸೈನ್ ಅಪ್ ಮಾಡುವಂತೆ ಜನರಿಗೆ ಒತ್ತಾಯಿಸಿ.
4. ಭಾಗವಹಿಸುವವರು ಮಾತ್ರ ಹೋಸ್ಟಿಗೆ ಮೆಸೇಜ್ ಕಳುಹಿಸಬಹುದಾದ ರೀತಿಯಲ್ಲಿ ಚಾಟ್ ಸೆಟ್ಟಿಂಗ್ ಅನ್ನು ಹೊಂದಿಸಿ.
5. ಪ್ರತಿಯೊಂದು ಸಭೆಗೂ ಹೊಸ ಮೀಟಿಂಗ್ ಐಡಿ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್ ಒದಗಿಸಿ.
6. ಹೋಸ್ಟಿಗೆ ಮೊದಲು ಜಾಯಿನ್ (ಸಭೆಗೆ ಸೇರ್ಪಡೆಯಾಗಿ) ಅನ್ನು ಕಾರ್ಯಹೀನಮಾಡಿ.
7. ಹೋಸ್ಟ್ ಮೂಲಕ ಮಾತ್ರ ಸ್ಕ್ರೀನ್ ಷೇರ್ ಆಗುವಂತೆ ಅನುಮತಿಸಿ.
8. "ಹೊರತೆಗೆದ ಭಾಗಿದಾರರನ್ನು ಮರುಸೇರಲು ಅನುಮತಿಸು" ಅನ್ನು ಕಾರ್ಯಹೀನಗೊಳಿಸಿ.
9. ಎಲ್ಲಾ ಭಾಗಿದಾರರು ಸೇರಿದ ನಂತರ ಮೀಟಿಂಗ್ ರೂಮನ್ನು ಲಾಕ್ ಮಾಡಿ.
10. ಮೀಟಿಂಗ್ ರೆಕಾರ್ಡಾಗುವಂತಿದ್ದರೆ ಎಲ್ಲ ಭಾಗಿದಾರರಿಗೆ ತಿಳಿಸಿ.
11. ಬಳಸುವ ಜೂಮ್ ಕ್ಲೈಂಟ್ ಯಾವಾಗಲೂ ಇತ್ತೀಚಿನ ಆವೃತ್ತಿಯಲ್ಲಿ ನವೀಕೃತವಾಗಿದೆಯೆಂಬುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

http://164.100.117.97/WriteReadData/userfiles/comprehensive-advisory-Zoom-%20meeting%20platfom-20200412-(2).pdf ನಲ್ಲಿ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ನ ಸುರಕ್ಷಿತ ಬಳಕೆಗಾಗಿ ಗೃಹ ಸಚಿವಾಲಯವು ಸೂಚಿಸಲಾದ ಸೆಟ್ಟಿಂಗ್‌ಗಳ ಒಂದು ಸಮಗ್ರ ಪಟ್ಟಿಯನ್ನು ನೀಡಲಾಗಿದೆ.

ಉಲ್ಲೇಖಗಳು

1. ಜೂಮ್‌ನಲ್ಲಿನ ವಿಪತ್ತು ಸಾಧ್ಯತೆಗಳ CERT-In ಸಲಹೆ - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0011
2. ಜೂಮ್‌ನಲ್ಲಿ ಸುರಕ್ಷಿತ ಸೆಟ್ಟಿಂಗುಗಳ ಬಗ್ಗೆ CERT-In ಸಲಹೆ - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0010
3. ವೆಬ್ ಕಾನ್ಫರೆನ್ಸಿಂಗ್ ಮಾಡುವಾಗ ಅತ್ಯುತ್ತಮ ಅಭ್ಯಾಸಗಳ ಬಗ್ಗೆ CERT-In ಸಲಹೆ - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0020
4. ವಿಂಡೋಸ್ ಮತ್ತು MacOS ಗಳ ಜೂಮ್ ಕ್ಲೈಂಟ್‌ನಲ್ಲಿ ಗುರುತಿಸಲಾಗಿರುವ ಹಲವು ಸೆಕ್ಯುರಿಟಿ ವಿಪತ್ತುಗಳು - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0011
5. ಜೂಮ್‌ನ iOS ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ಸಂಬಂಧಿಸಿದ ಸಮಸ್ಯೆಗಳು - https://www.msn.com/en-gb/money/technology/video-calling-app-zooms-ios-version-is-sharing-user-data-with-facebook/ar-BB11LEvv
6. ಜೂಮ್ ಸಂಪರ್ಕದ ದುರ್ಬಲ ಎನ್ಕ್ರಿಪ್ಷನ್ - https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
7. ಜೂಮ್‌ಗೆ ಸಂಬಂಧಿಸಿದ ಇತರ ಸಮಸ್ಯೆಗಳು - https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/?fbclid=IwAR3GdjDfhoEhtEmaWQOBmwpcVHNraW4falDl-AQBMxxxplEYH3amoYY0T18

8. ಜೂಮ್‌ನ ಸುರಕ್ಷಿತ ಬಳಕೆಗಾಗಿ ಶಿಫಾರಸಾದ ಸೆಟ್ಟಿಂಗ್‌ಗಳು - https://twitter.com/BostonJoan/status/1243923595874783232

CySecK Advisory -

Usage of Zoom for online meetings

Published on: 17-April-2020

Advisory Summary

Multiple security and privacy issues have been identified on Zoom online meeting / webinar platform. Based on these issues, the following are recommended.

1. Government officers / offices are advised not to use Zoom for online meetings.
2. Private individuals / enterprises are recommended to avoid Zoom for any meetings discussing confidential / secret matters. If you have purchased Zoom licenses, you can continue using it for the duration of investment for non-secret meetings.
3. Private individuals / enterprises using Zoom should review the settings on the platform and follow the best practices.
4. Advise all users to update the Zoom client on their systems to the latest version.

Key recommended settings

The below are key settings recommended to be configured on the Zoom platform.

1. Use the waiting room feature of Zoom so that host(s) need to explicitly let in attendees after they login and before they enter the meeting.

2. Configure the settings so that calls begin with video and audio muted by default and only the host(s) can control who will be allowed to speak / share video.
3. Insist on people signing up to Zoom account with recognisable name, so that intruders can be identified easily.
4. Set the chat setting so that participants can only message the host.
5. Set new meeting id and password for each meeting.
6. Disable join before host.
7. Allow screen sharing by host only.
8. Disable “Allow removed participants to re-join”.
9. Lock meeting room once all attendees have joined.
10. Inform all attendees if the meeting is recorded.
11. Ensure Zoom client used is always kept updated to the latest version.

Ministry of Home Affairs has provided a comprehensive list of suggested settings for secure usage of the platform at http://164.100.117.97/WriteReadData/userfiles/comprehensive-advisory-Zoom-%20meeting%20platfom-20200412-(2).pdf

References

1. CERT-In advisory regarding vulnerabilities on Zoom - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0011
2. CERT-In advisory regarding secure settings for Zoom - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0010
3. CERT-In advisory regarding generic best practices while web conferencing - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0020

4. Multiple security vulnerabilities identified on Zoom client for Windows and MacOS - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0011
5. Concerns related to Zoom's iOS app - https://www.msn.com/en-gb/money/technology/video-calling-app-zooms-ios-version-is-sharing-user-data-with-facebook/ar-BB11LEvv
6. Weak encryption of Zoom communication - https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
7. Other concerns related to Zoom - https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/?fbclid=IwAR3GdjDfhoEhtEmaWQOBmwpcVHNraW4falDl-AQBMxxxplEYH3amoYY0T18
8. Recommended settings for secure usage of Zoom - https://twitter.com/BostonJoan/status/1243923595874783232