CYBER SECURITY ADVISORY – ZOOM

April 9, 2020

EXECUTIVE SUMMARY

You are receiving this advisory to make you aware of security issues and vulnerabilities that are being actively exploited in Zoom conferencing software.

It is strongly recommended that organizations that have or use Zoom, update to the latest supported and patched versions, follow best practices and additional recommendations listed in this advisory.

HOW DOES THIS INCIDENT AFFECT MY ORGANIZATION?

Social distancing measures put in place to manage the pandemic have resulted in an increased number of employees working offsite. This shift is accompanied by an increased use of online conferencing tools such as Zoom that enable teams to collaborate and meet remotely. Zoom is one of the user-friendly online conferencing tools that has seen a vast increase in its userbase over the last few weeks (535% rise in daily traffic to the Zoom domain over the past month).

Because of its popularity and wide use, Zoom is targeted by threat actors who actively exploit improperly configured and insecure sessions. Recommendations to mitigate these risks are available and Zoom users are strongly encouraged to follow them.

WHAT SHOULD I DO?

As soon as possible, forward this notification to your cyber security personnel or IT partners for immediate action.

TECHNICAL DETAILS:

Zoom has been in the news because of concerns regarding privacy and security issues, including reports of Zoom meetings being interrupted by unauthorized users leveraging a technique called “Zoombombing”, in which threat actors access Zoom meetings without passwords, hijack them, and display inappropriate content.

“Zoombombing” is possible because users are not using available security measures for their meetings, such as passwords, and because users expose meeting codes and access information on social media. Also, Zoom uses meeting IDs that can be enumerated using available online tools, making it trivial for threat actors to access Zoom meetings that are not password protected.

Other concerns include a serious and recently patched vulnerability that can result in: leaked Windows Active Directory credentials; a privacy leak with Zoom's "Company Directory" setting; Zoom sending analytical data to Facebook; the strength of Zoom's encryption; and the fact that Zoom lacks end-to-end encryption.

Zoom has paid plans that offer additional features. it should be noted that the paid versions of Zoom (Pro, Business and Enterprise) allow for the ability to record Zoom conferences from the Zoom application itself. The Business and Enterprise versions of Zoom also allow for the ability to host all your conference data on your own private server as opposed to on a sever owned and operated by Zoom. This latter option would ensure that Zoom would not be able to access your content.

RECOMMENDED ACTION:

- Update to the latest supported version of Zoom
- Consider not using Zoom to host meetings that are expected to involve sensitive information. If you absolutely must use Zoom for sensitive conferences, consider using the Business or Enterprise versions of Zoom to take advantage of the feature allowing you to host conference data on your own server
- Add a strong password to ALL meetings and use the Waiting Room feature
- Ensure users are not exposing meeting ID's or passwords on Social Media
- Consider configuring Zoom to only allow the meeting host to share their screen
- Lock meetings when all participants have joined
- Be mindful of phishing messages impersonating Zoom meeting invites
- Be mindful that conference participants can potentially record video and audio of conferences
- Validate that you are following your teleconferencing software's security features and that it is configured correctly

NIST guide to Preventing Eavesdropping and Protecting Privacy on Virtual Meetings:
https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings

Zoom guide to meeting and Webinar Passwords:
https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords-

FBI warning:
https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic/layout_view

FOR FURTHER INFORMATION

The Cyber Security Division hosts a monthly Community of Practice call for the Broader Public Sector to discuss Cyber Security topics and issues. The call is open to any Broader Public Sector organization wishing to participate. Contact cyberadvice@ontario.ca to be added to the invite list. The frequency of these calls has been increased from monthly to weekly for the duration of the pandemic with a focus on COVID-19 related Cyber Security issues.

CYBER SECURITY ADVISORY – ZOOM

If you find any of the indicators of compromise (IOCs) on your networks, have related information or any questions, please contact cyberadvice@ontario.ca

NO WARRANTY
This Cyber Advisory contains third party content and links. CS CoE does not control or maintain third party links and makes no representation or warranty that the link will still work when you click on it or the service or content is useful, appropriate, virus-free or reliable. It is your responsibility to determine whether you want to follow any link or agree to receive or rely on any service or content that is made available to you.

Cyber Security CoE is providing information about a known threat for potential use at the sole discretion of recipients to protect against cyber threats. This notification is provided to help broader public service organizations enable cyber preparedness and resilience.

DEFINITIONS:
Cyber Security Threats or Incidents are events that may present risk to the security (i.e. confidentiality, availability or integrity) of an organization's information assets, systems and networks.

- Cyber Security THREAT Advice is issued when NO ACTIVE EXPLOITS are observed. Purpose of the advice: to enable organizations to prepare for and mitigate cyber threats.
- Cyber Security INCIDENT Advice is issued when an ACTIVE EXPLOIT is observed. Incident advice is time sensitive to inform partner organizations of an ongoing cyber incident for a timely response and remediation.