CERTuy
CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

agesic
DESARROLLANDO EL URUGUAY DIGITAL

Uruguay **Presidencia**

Recomendaciones para la adopción de software de videoconferencias

1 Resumen ejecutivo

Debido a la pandemia generada por el coronavirus COVID-19, se ha establecido una cuarentena generalizada en varios países. Por esta razón y con el objetivo de mantener el ritmo de trabajo y los servicios usuales, se ha incrementado el uso de herramientas colaborativas remotas, en particular, el uso de las videoconferencias para remplazar las reuniones presenciales.

Es habitual que tanto las herramientas de software como las plataformas online tengan un análisis exhaustivo de seguridad por parte de usuarios o agentes externos; esta actividad se incrementa notablemente junto con la popularidad de la plataforma. Debido a que actualmente la demanda de herramientas de trabajo remoto se ha incrementado, es esperable que se incremente el reporte de vulnerabilidades y debilidades de las distintas plataformas disponibles.

En particular, la herramienta Zoom cuenta con un amplio abanico de tipos de usuarios y una gran popularidad de uso. La facilidad de uso para usuarios no técnicos y la falta de configuraciones de privacidad activadas por defecto han repercutido a nivel mediático en forma negativa, generando una percepción de riesgo elevada. Es por esto que haremos un análisis más detallado de la herramienta y cómo se la puede usar de manera segura, siendo esta una alternativa válida siempre que no sea utilizada para el desarrollo de temáticas de información sensibles.

2 Objetivo

Analizar ventajas y riesgos asociados al uso de soluciones para videoconferencia, haciendo un especial énfasis en Zoom por ser una de las soluciones más difundidas.

Proveer un conjunto de recomendaciones generales para el uso de herramientas de videoconferencias.

En este documento solo se analizan algunas herramientas de videoconferencia y no necesariamente herramientas de trabajo colaborativo.

3 Público objetivo

El presente documento está destinado a personas que cuenten con conocimientos técnicos informáticos.

4 Soluciones para videoconferencia

En esta sección se intenta comparar diversas alternativas de herramientas para la realización de videoconferencias, a partir de sus puntos fuertes; se excluye el concepto de precio.

Las soluciones planteadas se seleccionaron en base a su similitud con otras comparativas disponibles en los últimos meses. Si bien existen otras también populares que podrían introducirse en la comparación, se optó por las siguientes dado que no es necesario vincular la cuenta de la herramienta de videoconferencias con servicios de autenticación de otras plataformas, requiriéndose solamente una casilla de correo para realizar la validación durante la creación de la cuenta.

Dentro de las soluciones comparadas, se hizo foco en su política de seguridad y sus características de seguridad.

	Cisco Webex	GoToMeeting	ClickMeeting	Zoom	Wire	Jitsi
Compartir contenido	✓	✓	✓	✓	✓	✓
Salas protegidas por contraseñas OTP	✓	×	×	×	✓	×
Cliente multiplataformas	×	✓	N/A	✓	✓	✓
Cifrado punto a punto	✓	✓	✓	✓ *	✓	✓
Foco en seguridad y privacidad	✓	×	×	×	✓	✓
Instalación en infraestructura local **	✓	×	×	✓	✓	✓
Instalación full on-premises	×	×	×	×	×	✓
Open source	×	×	×	×	✓	✓
Soporte oficial	✓	✓	✓	✓	✓	×
Participación de usuarios externos	✓	✓	Solo espectador	✓	✓	✓

(*) Con las excepciones anteriormente descriptas.

(**) Permite, entre otras funcionalidades, autenticar contra un servidor de autenticación local.

Referencias:

- https://wire.com/en/security/
- https://www.webex.com/products/it_buyer.html/
- https://knowledge.clickmeeting.com/privacy-security/
- https://gotomeeting.com/download/security-white-paper
- https://zoom.com/security

5 Análisis de Zoom

Varias de las decisiones y características de usabilidad que hacen que esta herramienta sea muy fácil de utilizar por distintos tipos de usuarios con distinto niveles de conocimiento técnico hacen también que esta sea propensa a la falta de ajustes en las configuraciones de privacidad y seguridad por parte de los usuarios

A continuación, se describen algunas de las razones por las cuales la herramienta está siendo cuestionada tanto a nivel de seguridad como de privacidad.

5.1 Vulnerabilidades y riesgos de seguridad

1. **Inyección de contenido o "Zoombombing":**
   a. **Riesgo**: Consiste en la interrupción no consentida de una sesión de videoconferencia debido al envío de imágenes y otro contenido ofensivo no relacionados a la temática tratada; esto ocurre, principalmente, debido a la mala configuración de la sesión, cuando esta es generada con acceso público y sin clave, entre otros aspectos.
   b. **Mitigación**: Realizar configuraciones de privacidad, contraseña de videollamada y sala de espera.
   c. Un caso conocido del problema citado es el de inyección de contenido a diputados de USA (ver referencia).
2. **Explotación de rutas UNC:**
   a. **Riesgo:** Permite al atacante inyectar en el chat rutas a archivos internos en un equipo comprometido o un equipo malicioso; de esta forma, es posible hacerse con credenciales NTLM de la víctima, como ha sido demostrando en PoC
   b. **Mitigación:** Esta vulnerabilidad ya fue parcheada por el equipo de Zoom, por lo que es necesario actualizar el software a su última versión desde la página del proveedor o la tienda de aplicaciones correspondiente.
3. **Escalamiento de privilegios "Zoom-Doom":**
   a. **Riesgo:** Permite a un atacante que cuente con acceso físico explotar una vulnerabilidad conocida en las librerías del cliente Zoom; de esta forma, se podría generar un acceso permanente al equipo vulnerado.
   b. **Mitigación:** Las librerías vulnerables ya fueron parcheadas, por lo cual es necesario mantener el cliente actualizado para mitigar esta vulnerabilidad.
4. **Exposición de datos/información sensible:**
   a. **Riesgo:**

i. **Zoom podría acceder al contenido de una videollamada**, aunque declara que "no tienen desarrollada esa capacidad". El equipo de Zoom cita: "*Zoom has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list*".
ii. **Falta de cifrado de videollamadas en ciertas condiciones**. Se aclara que el cifrado solo se da si se cumplen algunas condiciones:
    1. Todos los participantes usan un cliente de Zoom.
    2. No se está grabando la videoconferencia.

    El equipo de Zoom cita: "*To be clear, in a meeting where all of the participants are using Zoom clients, and the meeting is not being recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.*". Zoom solamente cifra el "video, audio, pantalla y chat" si:

b. **Mitigación:** La plataforma cuenta con un conjunto de funcionalidades que permiten incorporar participantes teléfono de línea convencional (PSTN); es esperable que este canal no cuente con cifrado incorporado. De manera similar, la opción de grabado y reproducción vía browser de videollamadas es otra de las justificaciones para no realizar cifrado del contenido. **Debido a los puntos anteriores, es necesario tener en consideración la confidencialidad de la temática tratada en las sesiones cuando se utiliza esta herramienta.**

5. **Fuga de información:**
    a. **Riesgo:** Fuga de información de cuentas de usuarios, correos electrónicos e información personal. Adicionalmente, se tiene conocimiento de venta de bases de datos de credenciales pertenecientes al servicio de Zoom, pero que fueron comprometidas debido al uso de credenciales repetidas entre otros servicios.
    b. **Mitigación:** No utilizar credenciales compartidas entre distintos servicios, mantener cuentas seguras y distintas por servicio.
6. **Pasaje de información por países donde no se comparte la misma legislación a nivel de información**
    a. **Riesgo:** Previamente, y debido a un problema de ruteo, se verificó que muchas de las comunicaciones se registraban a través de IP pertenecientes al segmento de China. Esto, vinculado con los controles que presenta el gobierno de China a nivel de información y/o noticias de espionaje, presenta una opción no muy segura a nivel de privacidad. Zoom ya ha dado testimonio al respecto, informando del error y generando la solución de forma pública.
    b. **Mitigación:** Considerar si Zoom es la herramienta adecuada si la confidencialidad de los datos tratados durante la sesión es de carácter sensible.
7. **Información pública de ID de sesión de Zoom**
    a. **Riesgo:** A través de Google y herramientas de *doxing,* es posible encontrar reuniones con ID publicas indexadas por el buscador de Google, permitiendo de esta forma realizar ataques de fuerza bruta y/o bombardeos a las salas.
    b. **Mitigación:** Hacer uso de ID de sesión aleatorios y no mantenerlos para sucesivas instancias; adicionalmente, invitar exclusivamente a los participantes y no informar de manera pública los datos de la sesión.
8. **Posible venta de *zero days***

a. **Riesgo:** Fueron encontrados dos anuncios, los cuales vendían dos *zero day* posteriores al parcheado realizado por Zoom. Estas brechas de seguridad serían del tipo RCE y afectarían a clientes MacOs, permitiendo al atacante ejecutar comandos remotos y tomar control sobre el equipo cliente. La interfaz de MacOS está permitiendo a los atacantes encontrar múltiples vulnerabilidades dado el nivel de privilegio que tienen algunos componentes de la misma. Si bien no es posible constatar la veracidad de estos anuncios, es necesario tomar en cuenta que Zoom se encuentra posicionada como primera dentro de las herramientas de videoconferencia, lo que la transforma en un objetivo claro para quien vende este tipo de *exploits*.
b. **Mitigación:** Si bien no es posible tomar medidas ante una vulnerabilidad antes de tener detalle de ella, se recomienda mantener el software actualizado y estar al día con las noticias con el boletín de seguridad de Zoom.

Referencias:

- https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic
- https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
- https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-macOS
- https://zoom.us/privacy
- https://threatpost.com/alleged-zoom-zero-days-for-windows-macos-for-sale-report/154846/
- https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
- https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/

5.2 Recomendaciones específicas

Este apartado busca describir las opciones más importantes a configurar en la herramienta Zoom para evitar un comportamiento indeseado, tanto voluntario como involuntario, por parte de los participantes.

Mantener el cliente actualizado: En el sistema operativo en donde se instaló la herramienta es necesario configurar la opción de “chequeo de actualizaciones automáticamente”. Específicamente para el caso de Linux, es necesario ir al sitio web de Zoom para obtener la última versión. Cabe destacar que no es una opción que ya venga habilitada por defecto.

a. Windows: En el cliente, ir a la opción “check for updates” y si hay una actualización disponible, se permitirá descargar.
b. Linux: Descargar última versión y ejecutar el instalador.
c. MacOS: En el cliente, ir a la opción “check for updates” y si hay una actualización disponible, se permitirá descargar.

Utilizar credenciales robustas: Dado que el usuario y la contraseña utilizados en el cliente son los mismos que se utilizarán en la versión web de la herramienta, es recomendable utilizar

claves únicas y que contengan un nivel de complejidad alto. Hay que tener en cuenta que si las credenciales son comprometidas, un atacante puede modificar las configuraciones de su cliente de Zoom a través del sitio web de la plataforma.

Configuraciones de la sesión de videollamada: Dependiendo de la modalidad de participación o el público que va a participar en la sesión, es posible identificar algunas características importantes a configurar

Control de acceso a la videollamada:

a. Sala de espera. Esta opción viene por defecto habilitada en la última versión de la aplicación; igualmente, es posible validar su estado utilizando el botón de "seguridad" --> "Habilitar sala de espera".
b. Proteger sala con contraseña. Al crear una reunión o agendar una nueva, es posible configurar desde "Opciones" que se solicite una clave para el ingreso a ella.

Verificar privacidad en dispositivos móviles: En cuanto al acceso mediante dispositivos móviles, es recomendable verificar que los permisos a la cámara, micrófono y almacenamiento no se encuentren otorgados de forma permanente, sino que estos se otorguen en el momento en que se necesiten.

Configuraciones de privacidad: En cuanto a la visibilidad de datos en las cuentas, es recomendable desactivar la visibilidad de los siguientes ítems:

a. Número de teléfono.
b. ID personal.

Configuraciones adicionales: Dependiendo del público al que esté orientada la reunión, es posible generar distintos tipos de restricciones; por ejemplo:

a. Impedir que los usuarios puedan enviarse mensajes privados.
b. Prevenir que los usuarios activen la cámara.
c. Prevenir que los usuarios puedan compartir contenido mediante la herramienta de compartir pantalla.
d. Es posible evitar el ingreso de usuarios antes del ingreso del administrador de la reunión.
e. Prevenir que los usuarios utilicen el micrófono.
f. Permitir el acceso únicamente a usuarios registrados.
g. Solicitar que ingresen un usuario al momento de ingresar a la sala para auditar los integrantes.
h. Es posible desactivar la opción de ingreso a través del navegador.

Referencias:

- https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf?zcid=1231
- https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/
- https://zoom.us/docs/en-us/childrens-privacy.html?zcid=1231

6 Recomendaciones generales

A continuación, se listan una serie de recomendaciones asociadas al uso de la videoconferencia como herramienta de trabajo, configuración y buenas prácticas asociadas, independientemente del fabricante del software.

- Descargar las aplicaciones desde las tiendas oficiales con el fin de evitar utilizar una versión maliciosamente modificada.
- Mantener actualizadas las aplicaciones de videoconferencia, tanto en su versión de escritorio como de celular.
- Utilizar las restricciones proporcionadas por la herramienta, tales como evitar que los participantes puedan escribirse entre sí, compartir pantalla o ingresar a la reunión sin previa aprobación por parte del organizador. Es recomendable tomarse un tiempo para evaluar todas las opciones que el software ofrece, para evitar tanto errores por parte de los invitados como acciones mal intencionadas.
- Utilizar “salas de espera” en donde se evita que los participantes puedan ingresar a la sala previo al comienzo de la reunión, incluso conociendo el identificador de sala.
- Utilizar un identificador de sala aleatorio y solicitar clave para el ingreso a ella. Evaluar la no utilización del mismo identificador de sala para sesiones futuras.
- Evitar acceder a URL y archivos compartidos por el chat de la sala si no existe seguridad de su procedencia y contenido.
- Si se opta por grabar la sesión, se debe mostrar claramente a todos los participantes tanto de manera visual como sonora.
- Evitar la distribución del identificador de sala o invitación a personas ajenas a la reunión.
- Considerar el uso de otras herramientas para el intercambio de información sensible; las aplicaciones de videoconferencia no *self-hosted* no deben considerarse un canal seguro.
- Tener en cuenta que es posible, si se graba la sesión, que los mensajes “privados/personales” entre invitados puedan llegar al organizador una vez finalizada la videoconferencia.
- Como moderadores debemos insistir que los participantes utilicen nombres reconocibles dentro de la sala y verificar que estos son quien dicen ser.
- Considerar los aspectos del ambiente donde se está realizando la videoconferencia, tales como personas, documentos o información a la vista, niños, etc. Algunas herramientas de videoconferencia ofrecen la posibilidad de distorsionar el fondo u utilizar uno virtual. Considerar no utilizar video si no es necesario y utilizar la opción de *mute* del micrófono cuando no se esté hablando.

- Al igual que cualquier otro servicio, la cuenta con la que utilice la aplicación de videoconferencia debe tener una clave segura y única (no compartida entre otros servicios).
- Leer los términos y condiciones del software utilizado para conocer qué tratamiento se le dará a nuestra información por parte del proveedor del servicio.

Referencias:

- https://www.welivesecurity.com/la-es/2020/04/14/seguridad-zoom-como-configurarla-manera-correcta/
- https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls
- https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/215-abstract-el-uso-de-zoom-y-sus-implicaciones-para-la-seguridad-y-privacidad-recomendaciones-y-buenas-practicas/file

7 Conclusión

Independientemente de la plataforma a utilizar, es imprescindible conocer sus capacidades, para que la configuración por defecto no genere situaciones o riesgos no deseados, especialmente si la información a manejar será de índole confidencial o sensible. En particular, Zoom ha demostrado dar una respuesta rápida a las vulnerabilidades encontradas, aun cuando está siendo objeto de ciberataques debido a su popularidad.