UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

BOLETÍN INFORMATIVO

Gestión de los Sistemas de Información y las Telecomunicaciones

Volumen 2, Número 4 - Agosto de 2021

VULNERABILIDADES EN APLICACIONES DE VIDEOCONFERENCIA

1 ZOOM

Considerada como una de las mejores plataformas para realizar videoconferencias[1], Zoom se destaca principalmente por aumentar la capacidad de participantes hasta 1000.

Desde el 2020 se han reportado seis vulnerabilidades relacionadas con las aplicaciones de escritorio. En **abril de 2021,** un equipo de ***hackers blancos*** encontró que era posible la Ejecución Remota de Código (**RCE,** por sus siglas en inglés) y así tomar control de la computadora[2]. A raíz de vulnerabilidades como esta, te recomendamos:

* Usar contraseña de acceso y salas de espera para controlar quién ingresa.
* Instalar actualizaciones a la aplicación de escritorio o móvil para garantizar que se tengan los últimos parches de seguridad.

2 MICROSOFT TEAMS

Microsoft® Teams se ha consolidado como la plataforma preferida para las empresas en Colombia[1], por funcionalidades como, almacenamiento de documentos, gestión de documentos y transferencia de archivos.

El pasado **15 de junio** se encontró una vulnerabilidad **(ya corregida)** generada en Teams por la pestaña de Microsoft Power Apps, en la cual un ciberdelincuente a través de una pestaña maliciosa de acceso rápido a una aplicación podría acceder a documentos y comunicaciones privadas[3]. Teniendo en cuenta lo anterior, te recomendamos:

* Mantener actualizada la aplicación de escritorio o móvil.
* Evitar incluir aplicaciones de terceros desconocidos.

3 GOOGLE MEET

Google Meet se considera más segura en comparación con las otras herramientas mencionadas, debido a que funciona a través de la web y de esta manera no es necesario que obtenga permisos de acceso directo al dispositivo en el que se usa.

Google ha trabajado desde el 2020 en medidas de seguridad para Meet, ya que se presentaron situaciones en las que principalmente ingresaban intrusos a las reuniones. Por lo tanto, te recomendamos:

* Deshabilitar la opción de acceso rápido en las reuniones que realices.
* Finalizar la llamada para todos los participantes cuando esta termine.
* Usar un fondo de pantalla cuando habilites tu cámara.
* Habilitar la gestión de anfitriones.

RECOMENDACIONES ADICIONALES DE SEGURIDAD

1. Evita descargar archivos en reuniones o salas de chat, ya que podrían comprometer tu dispositivo y tu información.

2. Anuncia a los participantes de la reunión antes de iniciar la grabación para que no compartan en pantalla, por el micrófono o el chat de texto información confidencial o sensible.

3. Evita abrir enlaces en los chats de usuarios desconocidos, podrían ser ataques de *phishing* (suplantación de identidad).

[1]Consultar publicación *El furor por el móvil y la videoconferencia permanece un año después de la llegada del coronavirus* publicado por el diario El País. [2]Consultar publicación *Zoom: encuentran vulnerabilidad con la que pueden tomar control de computadora* publicado por el INFOBAE de México. [3]Consultar publicación *Vulnerability in Microsoft Teams granted attackers access to emails, messages, and personal files* publicado por el portal The Daily Swig.

No te pierdas nuestros próximos boletines informativos que se publicarán en la página web

VIGILADO MINEDUCACIÓN - DISEÑO: RED DE DATOS UDNET - CORRECCIÓN DE ESTILO: SECCIÓN DE PUBLICACIONES