Múltiples fallos de seguridad en ZOOM

BCSC_ALERTA_fallos_seguridad_ZOOM

TLP:WHITE

www.basquecybersecurity.eus

Abril 2020

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se facilita a título meramente informativo y orientativo. En ningún caso el Basque Cybersecurity Centre será o podrá ser responsable solidaria o subsidiariamente, de cualesquiera responsabilidades, daños, pérdidas y costos sufridos o incurridos, directos o indirectos, fortuitos o extraordinarios que pudieran derivarse del uso de la información que en el mismo se contiene.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

La expansión del virus **COVID-19** a nivel mundial ha llevado al confinamiento en sus casas a millones de personas y ha convertido el teletrabajo en un recurso básico que facilita la continuidad de la actividad empresarial. Esta circunstancia, unida a las necesidades de comunicación de las personas con sus familiares y allegados y a las diferentes actividades comerciales o de entretenimiento, ha convertido en cuestión de semanas al software de videoconferencia **ZOOM** en uno de los más utilizados de su sector, habiendo aumentado **de 10 a 200 millones de usuarios diarios**, lo que ha supuesto un incremento del **535%** del tráfico diario sobre su página de descarga en el último mes.

Al mismo tiempo que ZOOM experimentaba este crecimiento, durante las últimas semanas también han aumentado masivamente sus **problemas de seguridad**, todos ellos derivados de prácticas de diseño descuidadas o implementaciones débiles de seguridad, según se ha podido conocer a raíz de las múltiples investigaciones llevadas a cabo por parte de especialistas en ciberseguridad. Es tal la situación que ciertos medios han llegado a referirse a ZOOM como un *"malware"* y no como lo que realmente es, un software para videoconferencias.

Algunos de los fallos localizados afectan directamente a la **privacidad** de sus usuarios y permiten obtener datos confidenciales sobre ellos tales como direcciones de correo electrónico, videos, transcripciones y notas compartidas, fotos, etcétera. Adicionalmente, según se afirma en las investigaciones realizadas a este respecto, no existe un cifrado de extremo a extremo real.

Cabe mencionar que el propio CEO y fundador de Zoom lanzó un comunicado el pasado 1 de abril en el que reconocía algunos de los errores, confirmaba la solución de otros y explicaba qué está haciendo la compañía de forma inmediata para solucionar todas las vulnerabilidades de su software. Por tanto, Zoom ya ha solucionado algunos de los fallos reportados. A continuación, se recopilan todos los problemas detectados en la aplicación Zoom hasta la fecha.

ANÁLISIS TÉCNICO

En primer lugar, la **política de privacidad** de Zoom fue objeto de crítica, puesto que la aplicación daba la posibilidad de recopilar datos sobre sus usuarios, incluyendo vídeos, transcripciones y notas compartidas, así como compartirlos con terceros para un posible beneficio personal. A consecuencia de ello, el pasado 29 de marzo Zoom endureció su política de privacidad, afirmando que no utiliza datos de las reuniones con fines publicitarios. Sin embargo, sí utiliza los datos con esa finalidad cuando un usuario visita sus sitios web de marketing, incluidas sus páginas de inicio **zoom.us** y **zoom.com**.

Por otro lado, se ha podido constatar que la aplicación para **iOS** de Zoom, al igual que otras aplicaciones que utilizan el SDK de **Facebook**, enviaba datos analíticos a la mencionada red social, incluso si el usuario no tenía una cuenta de Facebook vinculada. A día de hoy Zoom ya ha eliminado esta función.

Hasta el pasado 2 de abril, momento en el que Zoom eliminó permanentemente la funcionalidad, este software disponía de una función denominada ***"seguimiento de asistentes"*** que, cuando estaba habilitada, permitía al anfitrión de una reunión verificar si los participantes hacían clic fuera de la ventana principal de Zoom durante una llamada. No obstante, hay que señalar que un anfitrión de una reunión de Zoom puede leer mensajes de texto privados enviados durante la llamada siempre y cuando ésta se haya grabado localmente.

Adicionalmente, un investigador de seguridad independiente descubrió que Zoom utiliza una técnica *"sombría"* para instalar su aplicación en sistemas **Mac** sin que se requiera interacción alguna por parte del usuario, utilizando "*los mismos trucos que utiliza el malware para osx*", permitiendo así que la aplicación se instale sin que los usuarios hayan otorgado su consentimiento. El 2 de abril Zoom emitió una solución resolviendo este error.

Por otra parte, diferentes investigadores descubrieron un fallo en la versión de **Zoom para Windows** que evidenciaba que la aplicación era vulnerable a un ataque de **inyección de ruta UNC**. Esta vulnerabilidad podría permitir a un atacante remoto robar las credenciales de inicio de sesión de Windows de los sistemas vulnerables e incluso ejecutar comandos arbitrarios. El 2 de abril se emitió un parche que abordaba este fallo y otros dos errores que permitían a los atacantes obtener privilegios de root y acceder al micrófono y la cámara en **macOS**, dando la posibilidad de grabar reuniones.

Dentro del funcionamiento de la aplicación Zoom se localizó una función de **minería de datos** no revelada que combinaba automáticamente los nombres de los usuarios y las direcciones de correo electrónico con sus perfiles de **LinkedIn** cuando iniciaban sesión, incluso si eran anónimos o usaban un seudónimo en su llamada. En relación con esto, aquellos usuarios que se hubieran suscrito a un servicio denominado ***LinkedIn Sales Navigator*** podían acceder a los perfiles de LinkedIn de otros participantes de sus reuniones de Zoom sin que tuviesen conocimiento de ello o hubiesen prestado su consentimiento. Zoom ya ha deshabilitado esta función.

El medio de comunicación Vice reveló que Zoom estaba **filtrando las direcciones de correo electrónico y las fotografías de miles de usuarios**, permitiendo a su vez que usuarios ajenos y desconocidos intentasen iniciar llamadas entre ellos. Esto se debe a que los usuarios cuya dirección de correo utilice un mismo nombre de dominio (proveedores de correo electrónico no estándar diferentes a Gmail, Outlook, Hotmail o Yahoo!) se agrupan como si trabajaran para la misma empresa. Como solución Zoom ha incluido en lista negra estos dominios.

El 3 de abril de 2020 el Washington Post informó de lo sencillo que era **encontrar grabaciones de video realizadas en Zoom** al buscar el patrón común de nombres de archivos que el software aplica automáticamente. Estos videos se encontraron en recursos de almacenamiento de Amazon de acceso público. Los investigadores que reportaron el fallo crearon una nueva herramienta llamada ***"zWarDial"*** cuya función es buscar IDs de reuniones de Zoom abiertas, encontrando alrededor de **100 reuniones por hora sin contraseña** alguna.

Teóricamente Zoom utiliza **cifrado de extremo a extremo** para asegurar las comunicaciones, pero investigaciones recientes han demostrado que esto no es así. La compañía declaró que en una reunión en la que cada participante usa un cliente Zoom y que no se está grabando, todo tipo de contenido (vídeo, audio, pantalla compartida y chat) se cifra en el lado del cliente y nunca se descifra hasta que llega a los otros receptores. Pero, en caso de tener habilitados **servicios de valor agregado**, como la grabación en la nube, Zoom tiene acceso a las claves de descifrado, que actualmente mantiene en su nube. Esto también facilita que los *"piratas informáticos o una agencia de inteligencia del gobierno obtengan acceso a esas claves"*, según han afirmado expertos en seguridad.

Además, investigaciones posteriores descubrieron que el tipo de cifrado utilizado por Zoom es débil, dado que el audio y el vídeo en cada reunión de Zoom se cifran y descifran con un solo **AES-128** utilizado en modo **ECB** que se comparte entre todos los participantes. El uso del modo ECB no es recomendable porque los patrones presentes en el texto sin formato se conservan durante el cifrado. Como añadido, se han encontrado evidencias que señalan que las claves generadas para las operaciones criptográficas se entregan a los participantes a través de servidores en **China**, incluso cuando todos los participantes de la reunión y la compañía suscrita a Zoom están fuera de China. Sobre este tema, el propio **CEO** de Zoom, **Eric S. Yuan**, respondió indicando que, a consecuencia del periodo de alto tráfico, se han visto obligados a agregar capacidad de servidor rápidamente y *"por error"* agregaron sus dos centros de datos chinos a una larga lista blanca de recursos de respaldo, permitiendo que los clientes ubicados fuera de China se conectasen a ellos.

Por último, cabe mencionar una nueva forma de intrusión que ha sido denominada ***"Zoombombing"***, donde los atacantes aprovechan las reuniones abiertas o desprotegidas y las configuraciones predeterminadas deficientes para hacerse cargo del intercambio de pantalla y transmitir pornografía u otro material explícito. El **FBI** ha llegado a emitir una advertencia que insta a los usuarios a ajustar su configuración para evitar el secuestro de videollamadas. A partir del 4

de abril Zoom comenzó a habilitar la función ***"sala de espera"***, que permite al anfitrión controlar cuándo un participante se une a la reunión y exigir a los usuarios que ingresen una contraseña para evitar este tipo de abusos.

MITIGACIÓN / SOLUCIÓN

La compañía creadora de Zoom ha respondido en gran medida a todas las vulnerabilidades y errores de su aplicación de manera rápida y transparente, habiendo solucionado a día de hoy varios de los problemas destacados por la comunidad de seguridad. Además, los responsables de Zoom han anunciado un congelamiento de 90 días en el lanzamiento de nuevas funciones para *"identificar, abordar y solucionar problemas de manera proactiva".* Entre sus objetivos se encuentra realizar una revisión exhaustiva con expertos ajenos a Zoom y publicar un informe de transparencia que detalle la información relacionada con las solicitudes de datos, registros o contenido legal.

Es importante destacar que para un usuario habitual de Zoom es muy recomendable **pensar cuidadosamente qué necesidades de seguridad y privacidad necesita para cada llamada que realice**. En el caso de conversaciones casuales o para celebrar eventos sociales y organizar conferencias, la seguridad que Zoom implementa por defecto probablemente sea suficiente. En cualquier caso, si se requiere compartir información confidencial, en el mercado existen otras opciones que pueden proporcionar más garantías en este aspecto. Por último, la mayor parte de las investigaciones alientan a los usuarios a utilizar la **función de contraseña** para un mayor nivel de confidencialidad que la función *"salas de espera"* de Zoom. En el caso del ***"Zoombombing"*** se debe establecer una contraseña de reunión y bloquearla desde el momento en que todos los participantes se hayan unido a ella.

La Electronic Frontier Foundation (**EFF**) ha publicado una **guía practica específica para Zoom** con el fin de proteger lo máximo posible las llamadas a través de Zoom.

REFERENCIAS ADICIONALES

- ZOOM - A Message to Our Users
- Harden Your Zoom Settings to Protect Your Privacy and Avoid Trolls

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?