Si utilizas el software de videoconferencia Zoom en tu computadora Mac, debes tener cuidado, ya que cualquier sitio web que visites en el navegador puede encender tu cámara sin pedir permiso.

Cabe mencionar que si alguna vez instalaste el cliente Zoom en tu dispositivo y lo desinstalaste, un atacante remoto todavía puede activar tu webcam.

Zoom es una de las plataformas de reuniones más populares basadas en la nube que ofrece opciones de video, audio y pantalla compartida para los usuarios, permitiéndoles realizar seminarios web, impartir cursos en línea, impartir capacitación o unirse a reuniones virtuales en línea.

En un post de Medium publicado hoy, el investigador de seguridad cibernética, Jonathan Leitschuh, reveló detalles de una vulnerabilidad crítica que no ha sido parcheada (CVE-2019-13450), en la aplicación cliente de Zoom para computadoras Apple Mac, que de combinarse con un defecto por separado, podría permitir a los hackers ejecutar código arbitrario en los sistemas de destino de forma remota.

Jonathan informó responsablemente de la vulnerabilidad a la compañía hace más de 90 días, pero el equipo de Zoom no ha ofrecido ningún parche de seguridad adecuado, lo que puso en riesgo la privacidad y seguridad de su más de 4 millones de usuarios.

La vulnerabilidad aprovecha la función de hacer clic para unirse al popular software de conferencia que ha sido diseñado para activar de forma automática la aplicación Zoom instalada en el sistema, lo que permite a los participantes unirse rápidamente a una reunión de video por medio de su navegador web tan ponto como hacen clic en una invitación.

Jonathan descubrió que para ofrecer esta función, el software Zoom ejecuta un servidor web local en el sistema, en el puerto 19421, que «*inseguramente*» recibe comandos a través de los parámetros HTTPS GET y cualquier sitio web en el navegador abierto puede interactuar con él.

Para aprovechar esta vulnerabilidad, un atacante debe crear un enlace de invitación por medio de su cuenta en el sitio web de Zoom e insertado en un sitio web de terceros como una etiqueta de imagen o usar un iFrame y tratar de convencer a los objetivos que visiten ese sitio web.

> *«Al habilitar 'Participants: on' al configurar una reunión, descubrí que cualquier persona que se uniera a mi reunión tenía automáticamente su video conectado»,* dijo Jonathan.

Tan pronto como los usuarios de Mac con el cliente Zoom instalado en su sistema visiten el sitio web malintencionado, lanzará a la fuerza la app Zoom y encenderá su cámara web, exponiendo a los usuarios a los hackers.

> *«Esto podría estar incrustado en anuncios malintencionados, o podría usarse como parte de una campaña de phishing. Si en realidad fuera un atacante, probablemente invirtiera algo de tiempo para incluir también la lógica de puertos en aumento que el código en la ejecución de JavaScript en el sitio de Zoom»,* agregó el investigador.

Desinstalar el software no es suficiente para deshacerse del problema, ya que Jonathan explicó que la función de hacer clic para unirse también acepta un comando que reinstala automáticamente Zoom sin la intervención o el permiso de los usuarios.

Además de encender la cámara web, la vulnerabilidad también puede ser utilizada para que un ataque DoS sea dirigido a la computadora.

> *«Zoom terminó parcheando esta vulnerabilidad, pero todo lo que hicieron fue evitar que el atacante encienda la cámara de video del usuario. No deshabilitaron la*

> *capacidad de un atacante de unirse a una llamada a cualquier persona que visite un sitio malicioso»*, dijo Jonathan.

La vulnerabilidad afecta a la última versión de Zoom para Mac (4.4.4).

Además de Zoom, Jonathan también reveló la vulnerabilidad a los equipos de Chromium y Mozilla, pero como el problema no reside realmente en sus navegadores web, por lo que no hay mucho que puedan hacer las compañías.

Sin embargo, los usuarios aún pueden solucionar el problema, solo necesitan desactivar manualmente la configuración que permite que Zoom encienda automáticamente su cámara web cuando se una a la reunión.

Para esto, solo es necesario acceder a la ventana de configuración de Zoom y habilitar la opción *«Desactivar mi video al unirse a una reunión».*

Respuesta de Zoom a los hallazgos del investigador

En un comunicado publicado hoy, la compañía reconoció el problema, pero agregó que *«debido a que la interfaz de usuario del cliente Zoom se ejecuta en primer plano al momento del lanzamiento, sería evidente para el usuario que se uniera a una reunión sin querer y podrían cambiar sus ajustes de video o irse inmediatamente».*

Además, la compañía aseguró que no tienen *«ninguna indicación»* si los problemas reportados han sido explotados para violar la privacidad de cualquiera de sus usuarios.

Zoom también reconoció otras preocupaciones relacionadas con su software y afirmó que la vulnerabilidad local a la denegación de servicio (DoS) reportada por el investigador ya se había solucionado en mayo pasado, aunque la compañía dijo que no obligó a sus usuarios a actualizar porque es *«empíricamente una vulnerabilidad de bajo riesgo».*

La compañía también dijo que instala un servidor web de funcionalidad limitada cuando los usuarios instalan el cliente de Zoom para ofrecer la función de reuniones de un solo clic, lo que podría evitar que los usuarios hagan un clic adicional antes de unirse a cada reunión, pero no comentó por qué permanece el servidor instalado en la máquina local aún cuando un usuario elige desinstalar el software del cliente.