A pesar de los múltiples intentos de Zoom por hacer que su software sea seguro, después de parchear vulnerabilidades graves y anunciar la llegada del cifrado de extremo a extremo, que finalmente solo estaría disponible para usuarios que pagan, se han descubierto dos nuevas vulnerabilidades críticas.

Investigadores de seguridad cibernética de Cisco Talos, revelaron hoy dos vulnerabilidades críticas en el software Zoom, que permitirían a los hackers piratear los sistemas de participantes de chat grupal o un destinatario individual remotamente.

Ambas vulnerabilidades son de recorrido de ruta, que pueden explotarse para escribir o plantar archivos arbitrarios en los sistemas que ejecutan versiones vulnerables del software de videoconferencia para ejecutar código malicioso.

Según los investigadores, la vulnerabilidad CVE-2020-6109, residía en la forma en que Zoom aprovecha el servicio GIPHY, recientemente adquirido por Facebook, para permitir a sus usuarios buscar e intercambiar imágenes GIF mientras chatean.

Los investigadores aseguran que la aplicación Zoom no verificó si un GIF compartido se está cargando desde el servicio Giphy o no, lo que permite que un atacante incruste GIF desde un servidor controlado por terceros, que permitiría almacenar en el sistema de los destinatarios una carpeta específica asociada con la aplicación.

Además, debido a que la aplicación tampoco desinfectaba los nombres de los archivos, podría haber permitido a los atacantes lograr el recorrido del directorio, engañando a la aplicación para que guarde archivos maliciosos disfrazados como GIF en cualquier ubicación del sistema de la víctima, por ejemplo, la carpeta de inicio.

La segunda vulnerabilidad de ejecución remota de código, CVE-2020-6110, residía en la forma en que las versiones vulnerables de los fragmentos de código de proceso de la aplicación Zoom se compartían a través del chat.

> *«La funcionalidad de chat de Zoom se basa en el estándar XMPP con extensiones adicionales para admitir la rica experiencia del usuario. Una de esas extensiones admite una función que incluye fragmentos de código fuente que tienen soporte para resaltar la sintaxis completa. La función para enviar fragmentos de código requiere la instalación de un complemento adicional, pero recibirlos no. Esta característica se implementa como una extensión del soporte para compartir archivos»,* dijeron los investigadores.

La característica crea un archivo zip del fragmento de código compartido antes de enviarlo y después lo descomprime de forma automática en el sistema objetivo.

Según los investigadores, la función de extracción del archivo zip de Zoom no valida el contenido del archivo antes de extraerlo, permitiendo de este modo que el atacante logre plantar binarios arbitrarios en computadoras específicas.

> *«Además, un problema de recorrido parcial de la ruta permite que el archivo zip especialmente diseñado escriba archivos fuera del directorio generado aleatoriamente»,* dijeron los investigadores.

Los investigadores de Cisco Talos probaron las vulnerabilidades en la versión 4.6.10 de la aplicación cliente de Zoom y lo informaron responsablemente a la compañía.

Zoom corrigió ambas vulnerabilidades críticas con la actualización a la versión 4.6.12 de su software lanzada el mes pasado para computadoras Windows, macOS y Linux.