Una vulnerabilidad de día cero fue descubierta en el software de videoconferencia Zoom para Windows, que podría permitir a un atacante ejecutar código arbitrario en la computadora de una víctima con Windows 7 o anterior.

Para explotar exitosamente la vulnerabilidad, lo que un pirata informático debe hacer es engañar a un usuario de Zoom para que realice alguna acción típica, como abrir un documento recibido.

La vulnerabilidad fue descubierta por un investigador que informó a Acros Security, que posteriormente informó al equipo de seguridad de Zoom.

Aunque la falla está presente en todas las versiones compatibles del cliente Zoom para Windows, solo es explotable en sistemas operativos Windows 7 o anteriores, debido a algunas características específicas del sistema.

> *«Esta vulnerabilidad solo es explotable en Windows 7 y versiones anteriores de Windows. Probablemente también sea explotable en Windows Server 2008 R2 y versiones anteriores, aunque no lo probamos»*, dijo Mitja Kolsek, cofundadora de 0patch.

Aunque Microsoft finalizó el soporte oficial para Windows 7 en enero de este año, ese sistema sigue siendo muy utilizado por usuarios y organizaciones.

Los investigadores de Acros Security y de 0patch, desarrollaron un micro parche para todas las versiones de Zoom para Windows, comenzando desde la versión 5.0.3 hasta la 5.1.2, para abordar el problema de seguridad y lanzarlo gratuitamente hasta que Zoom Video Communications lance un parche de seguridad oficial.

Cuando un usuario habilita 0patch en su sistema, el código malicioso enviado por un atacante no se ejecuta cuando un usuario de Zoom hace clic en el botón *«iniciar video»*.

> *«Zoom Client presenta una funcionalidad de actualización automática bastante persistente que probablemente mantendrá a los usuarios domésticos actualizados a menos que realmente no quieran»*, dijo Kolsek.
>
> *«Sin embargo, a los administradores empresariales a menudo les gusta mantener el control de las actualizaciones y pueden quedarse atrás un par de versiones, especialmente si no se corrigieron errores de seguridad en las últimas versiones».*

Los investigadores de Acros Security también desarrollaron un exploit funcional de prueba de concepto para la vulnerabilidad, que ya compartieron con Zoom y que no publicarán hasta que la compañía solucione el problema.

Sin embargo, la compañía publicó una demostración de video de prueba de concepto para mostrar cómo se puede activar un exploit malicioso para la vulnerabilidad al hacer clic en el botón «Iniciar video» en el cliente de Zoom.

Hasta que Zoom libere una solución oficial para el problema, los usuarios pueden dejar de utilizar temporalmente el cliente Zoom en sus versiones anteriores de Windows, o actualizar el sistema a una versión más reciente.

También pueden implementar el micro parche lanzado por Acros Security, pero debido a que proviene de una compañía de software de terceros y no de Zoom, no es muy recomendable hacerlo.

Actualización

Zoom confirmó que ya parcheó la vulnerabilidad con el cliente Zoom versión 5.1.3.

> *«Los usuarios pueden ayudar a mantenerse seguros aplicando las actualizaciones actuales o descargando el último software de Zoom con todas las actualizaciones*

> *de seguridad actuales de https://zoom.us/download«.*