13/06/22

Ejecución de código remoto en Zoom sin que el usuario llegue a interactuar

Project Zero de Google ha publicado los detalles de una ejecución de código remoto que afecta a **Zoom** permitiendo la ejecución de código remota.

Debido a una serie de vulnerabilidades detectadas se puede realizar la explotación de ellas, pudiendo ejecutar código remoto en el ordenador de un usuario a través de un mensaje de chat, sin que este llegue a interactuar en ningún momento para llegar a ser comprometido.

Lista de CVEs utilizados para la explotación de la ejecución de código remoto:

- **CVE-2022-25235**: Fallo en *expat* en el análisis de XML no fiables.
- **CVE-2022-25236**: Fallo en *expat* al analizar XML no fiables.
- **CVE-2022-22784**: Fallo en el cliente de Zoom (versiones previas a la 5.10.0) en la que se explota el analizador de XML debido a un fallo pudiendo obtener ejecución de código remoto.
- **CVE-2022-22786**: Fallo en el cliente de Zoom de Windows (versiones previas a la 5.10.0) que permite al atacante bajar la versión del cliente a una menos segura.
- **CVE-2022-22787**: Fallo en los clientes de Zoom (versiones previas a la 5.10.0) que permiten validar el nombre de *host* durante un intercambio de petición permitiendo al atacante que el cliente se conecte a un servidor malicioso.
- **CVE-2022-22785**: Fallo en el cliente de Zoom en las distintas plataformas (versiones previas a la 5.10.0) en la que la el atacante puede realizar un ataque de *spoofing* a un usuario.

Zoom ha parcheado el cliente y el lado del servidor, quedando resuelto desde la versión 5.10.4

Este tipo de fallos nos hace recoredar la **importancia** de mantener nuestros sistemas actualizados. Ya que podemos ser víctimas de un ataque sin que lleguemos a realizar ninguna acción, simplemente porque el *software* pueda ser fácilmente vulnerado.