Se han descubierto múltiples vulnerabilidades de un clic en una amplia variedad de aplicaciones de software populares, que pueden permitir a un atacante ejecutar potencialmente código arbitrario en los sistemas de destino.

Los problemas fueron descubiertos por los investigadores de Positive Security, Fabian Bräunlein y Lukas Euler, y afectan a aplicaciones como Telegram, Nextcloud, VLC, LibreOffice, OpenOffice, Bitcoin/Dogecoin Wallets, Wireshark y Mumbie.

> *«Las aplicaciones de escritorio que pasan las URL proporcionadas por el usuario para ser abiertas por el sistema operativo son frecuentemente vulnerables a la ejecución de código con la interacción del usuario. La ejecución de código se puede lograr cuando se abre una URL que apunta a un ejecutable malicioso (.desktop, .jar, .exe…) alojado en un recurso compartido de archivos accesible en Internet (nfs, webdav, smb, …) o una vulnerabilidad adicional en el controlador URI de la aplicación abierta»*, dijeron los investigadores.

En otras palabras, las vulnerabilidades provienen de una validación insuficiente de la entrada de URL que cuando se abre con la ayuda del sistema operativo subyacente, conduce a la ejecución inadvertida de un archivo malicioso.

El análisis de Positive Security descubrió que muchas aplicaciones no pudieron validar la URL, lo que permitió a un adversario crear un enlace especialmente diseñado que apunta a un fragmento de código de ataque, lo que resulta en la ejecución remota de código.

Luego de la divulgación responsable, la mayoría de las aplicaciones lanzaron parches para remediar las fallas:

- Nextcloud: Corrigió el problema en la versión 3.1.3 de Desktop Client lanzada el 24 de febrero (CVE-2021-22879).
- Telegram: Problema informado el 11 de enero y solucionado mediante un cambio en el servidor el 10 de febrero.

- VLC Player: Problema informado el 18 de enero, con la versión parcheada 3.0.13 programada para su lanzamiento la siguiente semana.
- OpenOffice: Se solucionará en la siguiente actualización (CVE-2021-30245).
- Mumble: Corregido en la versión 1.3.4 lanzada el 10 de febrero (CVE-2021-27229).
- Dogecoin: Corregido en la versión 1.14.3 lanzada el 28 de febrero.
- Bitcoin ABC: Corregido en la versión 0.22.15 lanzada el 9 de marzo.
- Bitcoin Cash: Corregido en la versión 23.0.0 (actualmente en proceso de lanzamiento).
- Wireshark: Corregido en la versión 3.4.4 lanzada el 10 de marzo (CVE-2021-22191).
- WinSCP: Se corrigió en la versión 5.17.10 lanzada el 26 de enero (CVE-2021-3331).

> *«Este problema abarca múltiples capas en la pila de aplicaciones del sistema objetivo, lo que facilita que los encargados de mantenimiento de cualquiera puedan echar la culpa y evitar asumir la carga de implementar medidas de mitigación por su parte»*, dijeron los investigadores.

«Sin embargo, debido a la diversidad de sistemas cliente y sus estados de configuración, es crucial que todas las partes involucradas asuman una cierta cantidad de responsabilidad y agreguen su contribución en forma de medidas de mitigación», como la validación de URL y evitar que los recursos compartidos remotos sean automáticos.