Si utilizas LibreOffice debes actualizarlo nuevamente a la última versión 6.2.6/6.3.0 del software de código abierto, con el fin de abordar tres nuevas vulnerabilidades que podrían permitir a los hackers evitar parches para dos vulnerabilidades previamente tratadas.

LibreOffice es una de las alternativas de código abierto más populares a la suite Microsoft Office, y está disponible para sistemas Windows, Linux y MacOS.

Una de las dos vulnerabilidades, identificada como CVE-2019-9848, que LibreOffice intentó reparar el mes pasado fue una falla en la ejecución del código que afectó a LibreLogo, un script de gráficos vectoriales de tortuga programable que se envía por defecto con LibreOffice.

Esta falla permite que un atacante cree un documento malicioso que pueda ejecutar silenciosamente comandos Python arbitrarios sin mostrar ninguna advertencia a un usuario objetivo.

Aparentemente, el parche para dicha vulnerabilidad fue insuficiente, pues permitió a dos investigadores separados volver a habilitar el ataque explotando dos nuevas vulnerabilidades:

CVE-2019-9850: Descubierta por Alex Infür, la vulnerabilidad en LibreOffice existe debido a una validación de URL insuficiente que permite a los atacantes maliciosos eludir la protección agregada al parche CVE-2019-9848 y nuevamente desencadenar la llamada a LibreLogo desde los controladores de eventos de script.

CVE-2019-9851: Descubierta por Gabriel Masei, la falla reside en una función separada donde los documentos pueden especificar scripts preinstalados, al igual que LibreLogo, que se puede ejecutar en varios eventos de script globales como abrir documentos, etc.

El parche para la segunda vulnerabilidad (CVE-2018-16858), que LibreOffice lanzó en febrero pasado, se omitió con éxito, volviendo a habilitar el ataque transversal del directorio que podría permitir que documentos maliciosos ejecuten cualquier script desde ubicaciones

arbitrarias en el sistema de archivos de la víctima.

CVE-2019-9852: Descubierto por Nils Emmerich de ERNW Research GmbH, un ataque de codificación de URL podría permitir a los atacantes evitar el parche para el ataque transversal del directorio.

Al explotar con éxito estas tres vulnerabilidades, un atacante remoto puede ejecutar silenciosamente comandos maliciosos en una computadora objetivo al convencer a la víctima de que solo abra un archivo de documento creado con fines malintencionados.

Se recomienda a los usuarios de LibreOffice actualizar su software a la última versión parcheada 6.2.6/6.3.0 tan pronto como sea posible.