Si utilizas LibreOffice, debes tener mucho cuidado con los documentos que abras con el software en los siguientes días, pues el programa utilizado por millones de personas, tiene una grave vulnerabilidad de ejecución de código no parcheada que podría introducir malware en tu sistema.

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

A inicios de este mes, LibreOffice lanzó la última versión 6.2.5 de su software que aborda dos vulnerabilidades graves (CVE-2019-9848 y CVE-2019-9849), pero el parche para la primera vulnerabilidad se omitió, según informó el investigador de seguridad Alex Inführ.

Aunque Inführ no ha revelado más detalles sobre la técnica explotada para dicha vulnerabilidad, el impacto de la misma sigue siendo grave.

La vulnerabilidad CVE-2019-9848, que aún existe en la última versión de LibreOffice, reside en LibreLogo, un script de gráficos vectoriales de tortuga programable que se envía de forma predeterminada con LibreOffice.

LibreLogo permite a los usuarios especificar scripts preinstalados en un documento que se puede ejecutar en distintos eventos, como pasar el mouse.

Descubierta por Nils Emmerich, la falla podría permitir a un atacante crear un documento malicioso que ejecute silenciosamente comandos Python arbitrarios sin mostrar ninguna advertencia a un usuario objetivo.

> *«El gran problema aquí es que el código no está bien traducido y solo proporciona código de Python, ya que el código del script a menudo da como resultado el mismo código después de la traducción»,* dijo Emmerich.
>
> *«Utilizando formularios y el evento OnFocus, incluso es posible obtener la ejecución*

> *del código cuando se abre el documento, sin la necesidad de un evento al pasar el mouse»,* agregó.

La vulnerabilidad CVE-2019-9849, se puede solucionar instalando la última actualización disponible, de no ser así, podría permitir la inclusión de contenido arbitrario remoto dentro de un documento, aún cuando el *«modo oculto»* esté habilitado.

El modo oculto no está habilitado de forma predeterminada, pero los usuarios pueden activarlo para indicar a los documentos que recuperen recursos remotos solo de ubicaciones de confianza.

Inführ ya notificó al equipo de LibreOffice el problema de la omisión, pero hasta que el equipo libere un parche para corregir la omisión, se recomienda a los usuarios actualizar o reinstalar el software sin macros o sin el componente LibreLogo, siguiendo estos pasos:

- Abrir la configuración para iniciar la instalación
- Seleccionar la instalación «personalizada»
- Expandir «componentes opcionales»
- Hacer clic en LibreLogo y seleccionar «Esta función no estará disponible»
- Dar clic en siguiente y luego instalar el software