OpenOffice y LibreOffice, las principales alternativas gratuitas a Microsoft Office, tienen una vulnerabilidad que permite a un hacker ejecutar código malicioso de forma remota y controlar la computadora de la víctima.

Este problema afecta a las computadoras con sistema operativo Windows o Linux que tengan instaladas alguna versión de LibreOffice anterior a la 6.1.3 o la última versión de OpenOffice 4.1.6, según informó el Instituto Nacional de Ciberseguridad (INCIBE).

Los dos paquetes de software permiten la ejecución de tareas automatizadas conocidas como macros, programa que se ejecuta al abrir algún documento.

Mediante la ejecución de macros, el hacker puede crear un fichero malicioso que se podría ejecutar en la computadora de la víctima para poder acceder a su información personal.

Si utilizas alguna de las versiones mencionadas de los paquetes de ofimática, puedes evitar el problema actualizando a la versión 6.1.4 de LibreOffice en su sitio oficial.

Para el caso de OpenOffice, no se ha publicado algún paquete que corrija la vulnerabilidad. Sin embargo, el INCIBE recomienda *«renombrar o eliminar el fichero pythonscript.py ubicado en la ruta (OpenOffice 4program)».*