Si ejecutas un entorno de escritorio KDE en tu sistema operativo Linux, debes tener mucho cuidado y evitar descargar cualquier archivo .desktop o .directory por un tiempo.

Un investigador de seguridad cibernética reveló una vulnerabilidad de día cero sin parches en el marco de software de KDE que podría permitir que los archivos .desktop y .directory creados de forma malintencionada ejecuten silenciosamente código arbitrario en la computadora de un usuario, sin siquiera requerir que la víctima lo abra.

KDE Plasma es uno de los entornos de escritorio basados en widgets de código abierto más populares para Linux, cuenta con un entorno de escritorio predeterminado en muchas distribuciones de Linux, como Manjaro, openSUSE, Kubuntu y PCLinuxOS.

El investigador de seguridad Dominik Penner, quien descubrió la vulnerabilidad, contactó a The Hacker News, informando que existe una vulnerabilidad de inyección de comandos en el escritorio KDE 4/5 Plasma debido a la forma en que KDE maneja los archivos .desktop y .directory.

> *«Cuando se crea una instancia de un archivo .desktop o .directory, evalúa de forma insegura las variables de entorno y las expansiones de shell mediante KConfigPrivate::expandString() a través de la función KConfigGroup::readEntry()»*, dijo Penner.

Explotar esta falla, que afecta el paquete 5.60.0 de KDE Frameworks y versiones posteriores, es simple e implica algo de ingeniería social, ya que un atacante necesitaría engañar al usuario de KDE para que descargue uno de los archivos maliciosos antes mencionados.

> *«El uso de un archivo .desktop especialmente diseñado para un usuario remoto podría verse comprometido simplemente descargando y visualizando el archivo en su administrador de archivos, o arrastrando y soltando un enlace en los documentos o escritorio. Teóricamente, si podemos controlar las entradas de configuración y*

> *activar su lectura, podemos lograr la inyección de comandos/RCE»,* dijo el investigador.

Como prueba de concepto, Penner también publicó código de explotación para una vulnerabilidad junto con dos videos que demuestran exitosamente los escenarios de ataque que explotan la vulnerabilidad de inyección de comandos de KDE KDesktopFile.

Aparentemente, el investigador no informó acerca de la vulnerabilidad a los desarrolladores de KDE antes de publicar los detalles y las vulnerabilidades de PoC, dijo KDE Community al tiempo que reconoció la vulnerabilidad y aseguró a los usuarios que una solución está en camino.

> *«Además, si descubre una vulnerabilidad similar, es mejor enviar un correo a security@kde.org antes de hacerlo público. Esto nos dará tiempo para parchearlo y mantener a los usuarios seguros antes de que los malos intenten explotarlo»,* dijo KDE Community.

Mientras tanto, los desarrolladores de KDE recomendaron a los usuarios que *«eviten descargar archivos .desktop o .directory y extraer archivos de fuentes no confiables»* por un tiempo hasta que sea reparada la vulnerabilidad.