Una nueva vulnerabilidad en el sistema operativo Linux compromete la seguridad de tu información al tratar de utilizar Vim o Neovim.

Armin Razmjou, investigador de seguridad, descubrió una vulnerabilidad de ejecución de comando de sistema operativo arbitraria de alto riesgo (CVE-2019-12735) en Vim y Neovim, las dos aplicaciones de edición de texto de línea de comandos más populares y potentes que ya vienen preinstaladas en la mayoría de sistemas operativos basados en Linux.

El editor Vim permite a los usuarios crear, ver o editar cualquier tipo de archivo, incluyendo textos, scripts de programación y documentos.

Ya que Neovim es resultado de una bifurcación extendida de Vim, con una mejor experiencia de usuario, incluyendo complementos y GUI, la vulnerabilidad de ejecución de código también reside en esta aplicación.

Razmjou descubrió una falla en la forma en que el editor Vim maneja *«modelos»,* una característica que está habilitada por defecto para encontrar y aplicar de forma automática un conjunto de preferencias personalizadas mencionadas por el creador de un archivo cerca de las líneas de inicio y finalización del documento.

Aunque el editor solo permite un subconjunto de opciones en modelos (por razones de seguridad) y usa la protección de la caja de arena si contiene una expresión insegura, Razmjou reveló que al usar *«:source!»* se puede utilizar para omitir el sandbox.

Debido a esto, solo abrir un archivo de aspecto inocente especialmente diseñado con Vim o Neovim podría permitir a los atacantes ejecutar comandos en secreto en su sistema Linux y tomar el control remoto sobre él.

El investigador también lanzó dos prueba de concepto al público, una de las cuales demuestra un escenario de ataque en la vida real en el que un atacante remoto obtiene acceso a una cubierta inversa desde el sistema de la víctima tan pronto como abre un archivo en eso.

Los mantenedores de Vim (parche 8.1.1365) y Neovim (lanzado en v0.3.6), lanzaron actualizaciones para ambas utilidades para solucionar el problema, que los usuarios deben instalar tan pronto como sea posible.

Además de esto, el investigador también recomendó a los usuarios:

- Deshabilitar la función de modelos
- Deshabilitar «modelineexpr» para no permitir expresiones en modelos
- Usar el plugin «securemodelines», una alternativa segura a los modelos vim