El creador del editor de texto en formato de código abierto Notepad++ ha lanzado la actualización de seguridad Notepad++ 8.5.7 al público. Esta última versión aborda cuatro problemas de seguridad en el cliente y también introduce modificaciones.

Los usuarios actuales pueden aplicar la actualización seleccionando el ícono de interrogación en la interfaz de Notepad++ y luego eligiendo *«Actualizar Notepad++»* en el menú que se despliega. Los nuevos usuarios y aquellos que prefieran descargar la versión más reciente manualmente pueden encontrarla, como es costumbre, en el sitio web oficial del proyecto en GitHub. También se encuentra disponible la versión portátil en el sitio web del proyecto.

correcciones de seguridad

Estos problemas de seguridad fueron reportados al proyecto hace algún tiempo y se hicieron públicos recientemente. Uno de los problemas, CVE-2023-40031, tiene una gravedad alta, mientras que los otros tres problemas, CVE-2023-40036, CVE-2023-40164 y CVE-2023-40166, tienen una gravedad media.

El problema calificado como alto se trata de un desbordamiento de escritura en el montón de búfer en la función Utf8_16_Read::convert, que se encarga de las conversiones entre UTF8 y UTF16. Si se explota con éxito, este problema puede llevar a la ejecución arbitraria de código.

CVE-2023-40031 describe un problema de desbordamiento de lectura de búfer global. La carga de un archivo especialmente manipulado podría resultar en *«la lectura más allá de los límites de un búfer de objeto global asignado». El investigador de seguridad que reportó el problema sugirió que tenía el potencial de revelar «información de asignación de memoria interna».*

CVE-2023-40036 y CVE-2023-40164 también describen problemas de desbordamiento de búfer. Según el investigador, no está claro cuán explotables son estos problemas, pero podrían *«usarse para revelar información de asignación de memoria interna».*

Los cambios no relacionados con la seguridad en Notepad++ 8.5.7

Se ha firmado la aplicación uninstall.exe de Notepad++, lo que, por definición, representa una mejora en la seguridad.

Los otros cambios realizados son los siguientes:

- Se corrigió un posible escape de memoria al leer archivos UTF8-16.
- Se mejoró el rendimiento al arrastrar las pestañas mientras se muestra la lista de documentos.
- Se añadió una opción de advertencia para archivos Superrss de 2GB en la versión x64.
- Se solucionó un problema que desvinculaba documentos clonados después de reiniciar la aplicación.
- Se resolvió un problema de guardado de sesión de archivo cuando el archivo es de solo lectura.
- Se solucionó un problema que activaba archivos incorrectos después de cargar archivos de sesión.
- Se modificó el lema en el instalador.