Los desarrolladores de VeraCrypt, un software de cifrado multiplataforma y de código abierto, lanzaron públicamente la versión 1.24 del software el 6 de octubre.

Ghacks hizo una revisión de la versión beta de VeraCrypt 1.24 en marzo de este año, ahora, la versión final del software desbloquea la actualización para entornos de producción.

VeraCrypt no admite la actualización automática, por lo que si utilizas este software, será necesario descargar la última versión y realizar la actualización de forma manual. También es posible descargar una versión portátil, que resulta más práctica para muchos administradores.

La mayoría de los cambios de VeraCrypt 1.24 se aplican a la versión de Windows del cliente, pero existen otros que se aplican a todos, entre ellos Linux y Mac, además de otros exclusivos para estos últimos.

Entre los cambios para todos los clientes, VeraCrypt 1.24 aumentó la longitud máxima de la contraseña para volúmenes que no son del sistema a 128 bytes en la codificación UTF-8, mejoró el rendimiento del modo XTS en máquinas de 64 bits que usan SSE2, obteniendo una rapidez aproximadamente del 10 por ciento más rápida, según los desarrolladores. También se corrigió la detección de algunas características de la CPU.

Última versión de VeraCrypt

Los usuarios de Windows resultan beneficiados con muchos cambios, entre estos, mejoras en la seguridad. Esta nueva versión admite el cifrado de RAM en máquinas de 64 bits. La función está deshabilitada de forma predeterminada, por lo que para activarla, se debe hacer en Configuración > Preferencias > Más configuraciones > Opciones de rendimiento y controlador > Activar cifrado de claves y contraseñas almacenadas en RAM.

Al hacer esto, se agrega una sobrecarga del 10% en las CPU recientes y se desactiva la hibernación del cifrado del sistema, según los mismos desarrolladores.

Muchas mejoras de seguridad están activadas por defecto en la nueva versión. VeraCrypt está configurado para borrar las claves de cifrado del sistema de la memoria cuando la máquina se apaga o se reinicia, esto ayuda a mitigar ataques de arranque en frío. Las mitigaciones protegen la memoria de la aplicación contra ataques de memoria de usuarios que no son administradores.

Otra característica interesante de seguridad, es la opción de borrar todas las claves de cifrado almacenadas en la memoria si un nuevo dispositivo está conectado al sistema. Esta opción tampoco está habilitada predeterminadamente, se puede habilitar en Configuración > Preferencias > Más configuraciones > Configuración de cifrado del sistema > Borrar claves de cifrado de la memoria si se inserta un nuevo dispositivo.

Los gestores de arranque, MBR y UEFI, se han mejorado en esta versión. El gestor de arranque MBR determina el segmento de memoria del cargador de arranque de forma dinámica en la nueva versión, presentando una solución para un problema que afectó la creación de sistemas operativos ocultos en algunas unidades de estado sólido.

El gestor de arranque UEFI presenta una nueva opción de tiempo de espera para la entrada de contraseña, además de mejoras del disco de rescate, incluyendo una opción para iniciar el cargador original de Windows desde el menú.

Entre otras mejoras, se encuentra la opción para utilizar CPU RDRAND o RDSEED como fuentes de entropía adicionales para el generador aleatorio si está disponible. Los usuarios pueden habilitar la opción en Preferencias > Opciones de rendimiento y controlador > Usar generados aleatorio de hardware de CPU como fuente adicional de entropía.

Las versiones de Mac OS X y Linux cuentan con un nuevo parámetro –no-size-check que desactiva la nueva verificación del tamaño de almacenamiento disponible al crear contenedores de archivos.

Si quieres probar este software para encriptar tu disco duro o memoria USB, puedes ayudarte con este tutorial.

Puedes descargar VeraCrypt 1.24 en el sitio oficial.