Una vulnerabilidad grave en el software de cifrado Libgcrypt de GNU Privacy Guard (GnuPG), pudo haber permitido a los atacantes escribir datos arbitrarios en la máquina de destino, lo que podría conducir a la ejecución remota de código.

La vulnerabilidad, que afecta a las versión 1.9.0 de libgcrypt, fue descubierta el 28 de enero por Tavis Ormandy, de Project Zero, una unidad de investigación de seguridad dentro de Google dedicada a encontrar vulnerabilidades 0-day en sistemas de hardware y software.

Cabe mencionar que ninguna otra versión de Libgcrypt se ha visto afectada por dicha vulnerabilidad.

> *«Existe un desbordamiento de búfer en la pila en libgcrypt debido a una suposición incorrecta en el código de administración de búfer de bloque. El simple hecho de descifrar algunos datos puede desbordar un búfer de pila con datos controlados por el atacante, no se valida ninguna verificación o firma antes de que ocurra la vulnerabilidad»*, dijo Ormandy.

GnuPG abordó la vulnerabilidad rápidamente un día después de la divulgación, al mismo tiempo que instaba a los usuarios a dejar de utilizar la versión vulnerable. Se puede descargar la última versión en este enlace.

La biblioteca Libgcrypt es un conjunto de herramientas criptográficas de código abierto que se ofrece como parte del paquete de software GnuPG para cifrar y firmar datos y comunicaciones. Una implementación de OpenPGP se utiliza para seguridad digital en muchas distribuciones de Linux como Fedora y Gentoo, aunque no se usan tanto como OpenSSL o LibreSSL.

Según GnuPG, el error parece haberse introducido en la versión 1.9.0 durante su fase de desarrollo hace dos años, como parte de un cambio para *«reducir la sobrecarga en la función de escritura hash genérica»,* pero Google Project Zero lo detectó apenas la semana pasada.

Por lo tanto, todo lo que un atacante debe hacer para desencadenar la falla crítica es enviar a la biblioteca un bloque de datos especialmente diseñado para descifrar, engañando de este modo a la aplicación para que ejecute un fragmento arbitrario de código malicioso incrustado en él (también conocido como shellcode) o bloquee un programa que se basa en la biblioteca Libgcrypt.

> *«Aprovechar este error es simple, y por lo tanto, se requiere una acción inmediata para los usuarios de la versión 1.9.0. Los archivos tar 1.9.0 en nuestro servidor FTP han sido renombrados para que los scripts ya no puedan obtener esta versión»,* dijo Werner Koch, autor de Libgcrypt.