¿Qué es “HASHLIB”?

Actualmente cualquier proyecto que requiera el almacenamiento de datos de un usuario hace uso de uno o múltiples algoritmos para llevar a cabo un cifrado, que permite ocultar o proteger determinada información. En la mayoría de los sitios que requieren de un registro las contraseñas son cifradas y se almacena un *hash* (el resultado) en lugar del texto original.

Existen diversos y muy variados algoritmos para realizar dicha acción; esta entrada cubre la utilización del MD5 (*Message-Digest Algorithm 5*) y las familias SHA (*Secure Hash Algorithm*), BLAKE y SHAKE.

El módulo hashlib pertenece a la librería estándar y permite realizar cifrados directamente desde Python con los algoritmos BLAKE, SHAKE, SHA1, SHA224, SHA256, SHA384, SHA512 y MD5.

No hemos encontrado problemas de vulnerabilidad documentados en cuanto a la utilización de HASHLIB.

¿Qué es “FERNET”?

Fernet es una receta que proporciona cifrado simétrico y autenticación de datos. Es parte de la biblioteca de criptografía para Python, desarrollada por la Autoridad Criptográfica de Python (PYCA).

Hay una variedad de casos de uso diferentes para Fernet. Los ejemplos del mundo real incluyen:

- Apache Airflow: esta plataforma de supervisión y programación de flujos de trabajo implementa fernet para cifrar contraseñas tanto para la configuración de variables como para la configuración de conexiones. Esto ayuda a mantener las contraseñas a salvo de los atacantes.

- Overcloud de Red Hat: las claves de Fernet se pueden utilizar para proporcionar cifrado en Overcloud de Red Hat, que es el entorno de la plataforma OpenStack de la empresa para crear y administrar recursos de red en nubes públicas y privadas.

- Databricks: Fernet puede desempeñar un papel en la protección de la información de identificación personal junto con otras herramientas como Databricks. Esta información es apreciada por los piratas informáticos, por lo que es importante contar con mecanismos seguros de encriptación y autenticación como fernet para protegerla.

Vulnerabilidades documentadas de la librería FERNET de Python.

Inconvenientes en encriptación de archivos mayores a 2 Gb:

https://github.com/pyca/cryptography/issues/5615

https://security-tracker.debian.org/tracker/CVE-2020-36242

Nuestro código encripta un archivo y calcula su hash. Así como también lo compara para saber si el archivo ha sido o no modificado. Luego desencripta y comprueba el hash del archivo desencriptado con el hash del archivo sin encriptar.

Integrantes del grupo: Daniel Beato, Yoel Fernández, Ramiro Giandinoto.