Vulnerabilidades en librería libgcrypt de GPG

BCSC_Vulnerabilidades_Libgcrypt_GPG

TLP:WHITE

Febrero 2021

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

Tavis Ormandy, investigador del “Project Zero” de Google, una iniciativa centrada en identificar vulnerabilidades en software de uso extendido ha descubierto una vulnerabilidad crítica en la **versión 1.9.0 de la librería libgcrypt**, utilizada, entre otros, por la aplicación **GnuPG.**

La explotación de dicha vulnerabilidad permitiría la ejecución remota de código, mediante el procesamiento de un fichero especialmente diseñado para aprovechar el fallo.

La biblioteca Libgcrypt es una toolkit open source de criptografía que se integra como parte de GnuPG para el cifrado y firma de datos y comunicaciones. Es una implementación de OpenPGP y se utiliza para la seguridad digital en muchas distribuciones de Linux, como Fedora y Gentoo, aunque no es tan utilizada como OpenSSL o LibreSSL.

Según la información proporcionada por GnuPG, la vulnerabilidad parece haber sido introducida durante el desarrollo de la versión 1.9.0 hace dos años debido a un cambio para “reducir la sobrecarga detectada en la función de escritura de hash”.

El proyecto GnuPG ha corregido este fallo en el mismo día de su notificación, y ya está disponible la nueva versión 1.9.1 con dicha corrección aplicada. Desde GnuPG instan a los usuarios a la actualización de sus sistemas.

2. ANÁLISIS TÉCNICO

Esta vulnerabilidad crítica detectada en Libgcrypt implica un desbordamiento de buffer en el conocido como heap (zona de memoria que se reserva dinámicamente durante la ejecución de un programa), producido por un cálculo incorrecto en el número de bytes a copiar a un buffer de tamaño fijo que, bajo ciertas circunstancias, excede el tamaño máximo y posibilita sobrescribir memoria más allá del mismo.

```
155   {
156     copylen = inlen;
157     if (copylen > blocksize - hd->count)
158       copylen = blocksize - hd->count;
159
160     if (copylen == 0)
161       break;
162
163     buf_cpy (&hd->buf[hd->count], inbuf, copylen);
164     hd->count += copylen;
165     inbuf += copylen;
166     inlen -= copylen;
167   }
```

En la zona contigua al buffer desbordado, se encuentra un puntero a una función que es llamada posteriormente con parámetros conocidos. Una escritura parcial de esta función permite redirigir el flujo de ejecución sin tener que preocuparse de protecciones como ASLR (Address Space Layout Randomization) permitiendo saltar a código cercano dentro de la librería afectada.

```
(gdb) pt hd
type = struct gcry_md_block_ctx {
  byte buf[128];
  u64 nblocks;
  u64 nblocks_high;
  int count;
  unsigned int blocksize_shift;
  _gcry_md_block_write_t bwrite;
} *
```

3. MITIGACIÓN / SOLUCIÓN

Se ha liberado, por parte del proyecto GnuPG, la versión 1.9.1 de la librería Libgcrypt que corrige esta vulnerabilidad.

Se puede consultar la información asociada a esta versión y sus release notes en la siguiente publicación de GnuPG:

https://lists.gnupg.org/pipermail/gnupg-announce/2021q1/000456.html

En esa misma publicación se encuentran las instrucciones para la descarga de la versión corregida.

Desde el proyecto GnuPG instan a la actualización inmediata ya que es el único método de mitigación actualmente disponible.

4. REFERENCIAS ADICIONALES

- Una al Día Hispasec – Vulnerabilidad crítica en la librería libgcrypt de gpg
- Twitter @FiloSottile
- The Hacker News – Google discloses severe bug in Libgcrypt Encryption Library
- Project-Zero Google Issue 2145
- GnuPG Annouce Libgcrypt 1.9.1. released

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?