Vulnerabilidades de denegación de servicio en ImageMagick

ImageMagick es una herramienta con un conjunto de utilidades de líneas de códigos abierto lo cual sirven para mostrar, manipular y convertir imágenes, siendo capas de leer y escribir 200 formatos. Muchas aplicaciones Web como MediaWiki, phpBB o vBulletin, pueden usar ImageMagick para generar miniaturas. También es usado por otros programas para la conversión de imágenes.

En este sentido, para esta herramienta se han reportado tres vulnerabilidades, las cuales son consideradas de una alta gravedad. En todos los problemas reportados, se evidencia que los múltiples errores son debido a la función 'MagickCore/draw.c',esto puedo ocasionar que un atacante remoto podría provocar denegaciones de servicio a través de archivos de imágenes especialmente manipulados.

En el primer problema, con CVE-2016-4562, el error se debe al no calcular correctamente determinados datos de tipo entero, lo que causa un desbordamiento de memoria (desbornamiento de búfer). El segundo problema, con CVE-2016-4563, este error consiste en el momento en el cual se relacionan incorrectamente el valor 'BezierQuantum' con otros tipos determinados de datos, también en este se evidencia un desbordamiento de memoria.

Por último, con CVE-2016-4564, este error se ocasiona al no localizar correctamente el siguiente token en determinadas llamadas de la función, lo cual igualmente provoca un desbordamiento de memoria.

Este problema afecta a las versiones anteriores a 6.9.4-0 y anteriores 7x-7.0.1-2. Se recomienda actualizar a versiones superiores.

Fuente: http://unaaldia.hispasec.com

Actualización del kernel para Ubuntu Linux

Ubuntu ha publicado una actualización del kernel para la versión de Ubuntu 14.04 LTS con la cual se solucionan 10 nuevas vulnerabilidades que podrían ser aprovechadas por atacantes para provocar denegaciones de servicio, obtener información sensible o comprometer los sistemas afectados.

Los problemas corregidos residen en la obtención de información sensible a través del driver Ethernet Atheros L2 (CVE-2016-2117), obtención de información sensible o denegaciones de servicio por lecturas fuera de límite en OZMO USB sobre drivers de dispositivos wifi (CVE-2015-4004), una condición de carrera en TLB (Translation Lookaside Buffer) del kernel de Linux (CVE-2016-2069),denegación de servicio a través del controlador USB de dispositivo digitalizador GTCO (CVE-2016-2187) y desactivación de protección ASLR (Address Space Layout Randomization) (CVE-2016-3672).

Por otra parte una denegación de servicio local por uso después de liberar en el controlador USB CDC Network Control Model (CVE-2016-3951), una escritura fuera de límites en la implementación USB/IP podría permitir la ejecución remota de código arbitrario (CVE-2016-3955), fuga de información en las implementaciones de ANSI/IEEE 802.2 LLC type 2 Support (CVE-2016-4485) y en la interfaz socket de rutado netlink (rtnetlink) (CVE-2016-4486) y por último una denegación de servicio local en fs/pnode.c (CVE-2016-4581).

Fuente:http://unaaldia.hispasec.com

Actualizaciónes de seguridad para Google Chrome

Google ha publicado una actualización de seguridad para su navegador Google Chrome (versión 51.0.2704.79) para todas las plataformas (Windows, Mac y Linux) que en este caso es para corregir 15 nuevas vulnerabilidades. También ha publicado una actualización de seguridad para la versión del navegar 51.0.2704.13, esta también es para todas las plataformas (Windows, Mac y Linux) pero en este caso, esta corrige 3 vulnerabilidades, asiendo un total de 18 vulnerabilidades corregidas en el mes de Julio por parte de Google.

Como es habitual, Google no facilita información de todos los problemas corregidos. En esta ocasión, confirma la corrección de dieciocho (18) nuevas vulnerabilidades aunque únicamente facilita información de nueve (9) de ellas y clasifica dos como de gravedad alta y cinco de importancia media. Se solucionan problemas de seguridad encontrados a través del trabajo de seguridad interno, de auditoría interna, pruebas automáticas y otras iniciativas por investigadores externos .

Los problemas de gravedad alta corregidos residen en un salto de las políticas de mismo origen en Blink y bindings de extensiones. Por otra parte, de importancia media una fuga de información bindings de extensiones, usos después de liberar en extensiones y en Autofill, un fallo de filtrado de parámetros en DevTools y una lectura fuera de límites en Skia. Según la política de la compañía las vulnerabilidades anunciadas han supuesto un total de 26.000 dólares en recompensas a los descubridores de los problemas. Los CVE asociados a estas vulnerabilidades van del CVE-2016-1696 al CVE-2016-1702.

También del trabajo de seguridad interno, varias correcciones procedentes de auditoría interna, pruebas automáticas y otras iniciativas (CVE-2016-1703).

Como es habitual, esta actualización está disponible a través de Chrome Update automáticamente en los equipos así configurados o a través de "Información sobre Google Chrome" (chrome://chrome/).

Google chrome

Fuente:http://unaaldia.hispasec.com

Vulnerabilidad critica en LibArchive compromete cientos de aplicaciones

En la actualidad las mayoría de las aplicaciones que se utilizan a diario, en vez de incluir en su propio código todas las funciones necesarias para funcionar sin problema, hacen uso de una serie de librerías ya existentes, haciendo así que se puedan implementar fácilmente las funciones necesarias en ella. Sin embargo, a diferencia de que el código se encuentra en la propia aplicación, si utilizamos librerías de terceros y estas se ven afectadas por algún fallo de seguridad, automáticamente nuestra aplicación también se verá afectada. En esta ocasión es lo que ha ocurrido con LibArchive.

LibArchive es una librería de código abierto creada en 2004 para el proyecto FreeBSD y utilizada principalmente por herramientas de compresión y por diferentes sistemas operativos con el fin de permitir a los usuarios trabajar cómodamente con ficheros comprimidos, entre los formatos de archivos comprimidos mas utilizados están TAR, 7z, ZIP, RAR, RAR.

Recientemente, el departamento de seguridad de Cisco, Talos, detectó y reportó una serie de vulnerabilidades en esta librería que podían permitir a un atacante ejecutar código en la memoria, con permisos de administrador, simplemente engañando a un usuario para que ejecutara el fichero comprimido en cualquier aplicación que hiciera uso de esta librería.

Concretamente, estas vulnerabilidades en la librería de compresión podrían resumirse principalmente en 3: la primera vulnerabilidad CVE-2016-4300, la cual afecta a los ficheros 7Zip. La segunda vulnerabilidad CVE-2016-4301,la cual afecta a los ficheros Mtree y por ultimo la vulnerabilidad CVE-2016-4302, que afecta a los ficheros RAR.

Además de afectar a los compresores de archivos, también puede comprometer la seguridad de otras herramientas de software, por ejemplo, los antivirus que también utilizan esta librería para acceder a los datos comprimidos ya que, un simple escaneo de un fichero comprimido vulnerable puede permitir, igual que abrir el archivo con el compresor, ejecutar código malicioso en la memoria del sistema.

Como hemos dicho, LibArchive es una librería de código abierto, por lo que podemos acceder a este, y a sus últimas versiones (entre ellas la 3.2.1 que soluciona estas vulnerabilidades mencionadas) a través de GitHub.

Fuente:http://blog.segu-info.com.ar