PRESIDENCIA DEL CONSEJO DE MINISTROS

Oficina Nacional de GOBIERNO ELECTRÓNICO e INFORMÁTICA

BOLETIN DE SEGURIDAD DE LA INFORMACIÓN

Centro de Consulta e Investigación sobre Seguridad de la Información

Edición Nº 69/ 29 de Abril de 2008

Visite el Portal del Estado Peruano: www.peru.gob.pe

CONTENIDO

FUENTES

- Hispasec
- Clamav
- Cert
- ESET
- VSAntivirus

VULNERABILIDAD EN REALPLAYER

RealPlayer es empleado por millones de usuarios de Internet para reproducir archivos multimedia tanto de audio como de vídeo. El fallo ha sido destapado por Elazar Broad, investigador especializado en descubrir fallos en los controles ActiveX de algunas de las aplicaciones más extendidas.

El problema está causado por un desbordamiento en el componente ActiveX RealAudioObjects.RealAudio (rmoc3260.dll) versión 6.0.10.45, que podría permitir a un atacante sobrescribir en bloques de memoria de la pila basada en heap y modificar así ciertos registros. Esto podría ser aprovechado para hacer que, si se visita con Internet Explorer una página web especialmente manipulada, se ejecutase código arbitrario.

El problema podría afectar a todas las versiones de RealPlayer y su descubridor dice estar trabajando en una demo, así que es posible que en pocos días esté disponible un expoit público que haga uso de la vulnerabilidad para ejecutar código arbitrario de forma remota.

MÁS INFORMACIÓN:

- **Real Networks RealPlayer ActiveX Control Heap Corruption**
  http://archives.neohapsis.com/archives/fulldisclosure/2008-03/0157.html
- **14/01/2008 La última vulnerabilidad de Real Player, aprovechada para infectar sistemas**
  http://www.hispasec.com/unaaldia/3369
- **26/11/2007 Múltiples vulnerabilidades en RealPlayer 10.x y 11.x**
  http://www.hispasec.com/unaaldia/3320
- **26/10/2007 Múltiples vulnerabilidades en productos RealPlayer, RealOne y HelixPlayer**
  http://www.hispasec.com/unaaldia/3289
- **22/10/2007 Vulnerabilidad en RealPlayer permite ejecución de código**
  http://www.hispasec.com/unaaldia/3285

VULNERABILIDADES EN CLAMAV

ClamAV es un motor antivirus de código abierto muy popular en el mundo del software libre, empleado con frecuencia en servidores de correo derivados de UNIX a modo de defensa perimetral primaria.

Se han encontrado múltiples vulnerabilidades en Clam AntiVirus que podrían ser aprovechadas por un atacante remoto, o por ciertas muestras de malware, para causar una denegación de servicio o ejecutar código en un sistema vulnerable.

Las vulnerabilidades se basan en una gestión potencialmente peligrosa de archivos binarios comprimidos con distintas herramientas.

- La primera vulnerabilidad está causada por un error de límites en la función cli_scanpe(), incluida en libclamav/pe.c. Esto podría ser aprovechado para causar un desbordamiento de memoria intermedia basado en heap por medio de un ejecutable especialmente manipulado, empaquetado con Upack. Un atacante remoto, podría hacer que la aplicación dejase de responder (denegación de servicio) o ejecutar código arbitrario.
- La segunda vulnerabilidad, descubierta por iDefense, está causada por un error de límites al procesar los PE empaquetados con el protector de ejecutables PeSpin. Esto podría ser aprovechado para causar un desbordamiento de memoria intermedia basado en pila, permitiendo la ejecución arbitraria de código.

- La tercera vulnerabilidad está causada por un error no especificado al procesar archivos ARJ especialmente manipulados que podrían causar que ClamAV dejara de responder.

- IDefense ha reportado una cuarta vulnerabilidad similar a las anteriores que causada en este caso por un fallo al procesar los archivos PE binarios empaquetados con el compresor de ejecutables WWPack.

MÁS INFORMACIÓN:

- **Announcing ClamAV 0.93**
  http://lurker.clamav.net/message/20080414.161123.ba784ba8.en.html

- **Upack Buffer Overflow Vulnerability**
  https://www.clamav.net/bugzilla/show_bug.cgi?id=878

- **ClamAV libclamav PeSpin Heap Overflow Vulnerability**
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=686

- **ARJ: Sample from CERT-FI hangs clamav**
  https://www.clamav.net/bugzilla/show_bug.cgi?id=897

- **ClamAV libclamav PE WWPack Heap Overflow Vulnerability**
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=687

- **CERT-FI and CPNI Joint Vulnerability Advisory on Archive Formats**
  https://www.cert.fi/haavoittuvuudet/joint-advisory-archive-formats.html

CODIGOS MALICIOSOS EN SITIOS CONOCIDOS

Los ataques, que se están llevando a cabo, han afectado a más de medio millón de páginas Web, comprometiéndolas de tal forma, que las mismas son capaces de enviar malwares a quienes las visitan.

La mayoría de los sitios comprometidos son muy populares. La extensa lista incluye desde páginas de muchos organismos gubernamentales, como los del gobierno británico, hasta el sitio de las Naciones Unidas, entre muchos otros.

Lo único que se requiere para infectarse, es visitar una de estas páginas sin tener las últimas versiones actualizadas del sistema operativo, del navegador, o de otros programas como reproductores multimedia, etc.

La presencia de un producto antivirus que pueda ser capaz de reaccionar sin necesidad de una actualización de firmas, mediante la detección avanzada de códigos maliciosos utilizando técnicas heurísticas, es hoy día algo fundamental.

Si el usuario no tiene estas protecciones, mientras visualiza las páginas comprometidas, un código en JavaScript es inyectado y puede ser ejecutado si encuentra alguna de por lo menos ocho vulnerabilidades conocidas en aplicaciones de Windows.

MÁS INFORMACIÓN:

- **Sitios populares con código malicioso, el gran problema**
  http://www.vsantivirus.com/24-04-08.htm

- **Blogs de Yahoo utilizados para spam**
  http://www.eset.com.uy/eset/?subaction=showfull&id=1208991932&n=2

- **Riesgo elevado en la navegación por Internet**
  http://www.vsantivirus.com/21-04-08.htm

- **Servidor y cliente "colaboran" para infectar al usuario**
  http://www.eset.com.uy/eset/?subaction=showfull&id=1208648394&n=2

- **Importancia de las actualizaciones**
  http://www.eset.com.uy/eset/?subaction=showfull&id=1207955349&n=2

- **Los sitios demasiado populares también son peligrosos**
  http://www.eset.com.uy/eset/?subaction=showfull&id=1206400070&n=2

CONGRESOS Y SEMINARIOS DEL 2008
Mayo 27 al 29 de 2008 **IV Congreso Internacional de Seguridad Electronica (Brasil)** http://www.abese.org.br/cis2008/
Junio 18 al 20 de 2008: **VIII Jornada Nacional de Seguridad Informática ACIS 2008 (Bogotá - Colombia)** http://www.acis.org.co/index.php?id=1066
Junio 23 al 25 de 2008: **The 5th International Conference on Autonomic and Trusted Computing (Oslo - Noruega)** http://www.ux.uis.no/atc08/
Junio 25 al 27 de 2008: **Sexto Congreso Collaborative Electronic Communications and eCommerce Technology and Research CollECTeR Iberoamérica 2008 (Madrid - España)** http://www.collecter.euitt.upm.es/
Julio 9 al 11 de 2008: **XIV Jornadas de Enseñanza Universitaria de la Informática (Granada - España)** http://jenui2008.ugr.es/
Septiembre 2 al 5 de 2008: **X Reunión Española de Criptología y Seguridad de la Información RECSI 2008 (Salamanca - España)** http://www.usal.es/~xrecsi/
Septiembre 10 al 12 de 2008: **EATIS 2008 Euro American Conference on Telematics and Information Systems (Aracajú - Brasil)** http://eatis.org/eatis2008/

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION
CCISI
EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106