UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2007-026

Buffer overflow en el control ActiveX IERPCtl de RealPlayer

El cliente RealPlayer de RealNetwroks para Microsoft Windows contiene un buffer overflow de pila en el parámetro *playlist* pasado al cliente a través de un control ActiveX. Esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código de su elección utilizando una página Web creada de forma específica o mediante un mensaje de correo electrónico en formato HTML.

Fecha de Liberación:	24 de Octubre de 2007
Ultima Revisión:	25 de Octubre de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas Afectados

Sistemas Windows con:

- RealOne Player
- RealOne Player v2
- RealPlayer 10
- RealPlayer 10.5
- RealPlayer 11 beta

II. Descripción

RealPlayer de RealNetworks es una aplicación multimedia que permite a los usuarios visualizar contenido de audio y video de forma local y remota. RealPlayer para Microsoft Windows incluye el control ActiveX IERPCtl, el cual puede ser utilizado con Intenet Explorer para importar un archivo local a una lista de reproducción. RealPlayer no valida adecuadamente el parámetro playlist pasado desde el control ActiveX dando como resultado una vulnerabilidad de buffer overflow de pila. El control ActiveX IERPCtl está presente en RealOne Player y versiones posteriores.

RealNetworks ha liberado una actualización para esta vulnerabilidad como se describe en la *Vulnerabilidad de Seguridad de RealPlayer*. Existen reportes públicos de que la vulnerabilidad está siendo explotada activamente.

Esta vulnerabilidad puede ser explotada utilizando el control ActiveX IERPCtl, lo que significa que solo los usuarios de Internet Explorer de Windows son afectados. El control ActiveX fue introducido en RealOne Player, por lo que las versiones de Windows de RealPlayer 8 y anteriores no son afectadas. Las versiones de Macintosh y Linux de RealPlayer no son afectadas.

III. Impacto

Convenciendo a un usuario de que visualice un documento o un mensaje de correo en formato HTML creado de forma específica, un atacante remoto no autenticado podría ser capaz de ejecutar código de su elección con los privilegios del usuario en un sistema vulnerable. Note que el software de RealPlayer no necesita ser ejecutado para que esta vulnerabilidad sea explotada.

Para mayor información, consulte la Nota de Vulnerabilidad del US-CERT VU#871673.

IV. Solución

Actualizar la versión de RealPlayer y aplicar un parche

Consulte la *Vulnerabilidad de Seguridad de RealPlayer* para información sobre como actualizar y parchar RealPlayer. Los usuarios de RealPlayer 10.5 y RealPlayer 11 beta deberían instalar el parche especificado en el documento de RealNetworks. Los usuarios de RealOne Player, RealOne Player v2, y RealPlayer 10 deberían actualizar a RealPlayer 10.5 o RealPlayer 11 beta e instalar el parche.

Deshabilitar el control ActiveX IERPCtl

Deshabilite el control ActiveX IERPCtl estableciendo el kill bit para el siguiente CLSID:

{FDC7A535-4070-4B92-A0EA-D9994BCC0DC5}

Más información sobre como establecer el kill bit está disponible en el Documento de Soporte de Microsoft 240797. Alternativamente, el siguiente texto puede ser guardado como un archivo .reg e importado en el registro de

Windows:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\ActiveX

Compatibility\{FDC7A535-4070-4B92-A0EA-D9994BCC0DC5}]

"Compatibility Flags"=dword:00000400
```

Desactivar ActiveX

Desactivando ActiveX en la Zona de Internet (o cualquier zona utilizada por un atacante) reduce las opciones de explotar esta y otras vulnerabilidades. Las instrucciones para deshabilitar ActiveX en la Zona de Internet pueden ser encontradas en el documento *Asegurando tu navegador Web (en inglés)*.

V. Apéndice A. Información del distribuidor

RealNetworks

Para información sobre como actualizar RealPlayer consulte la *Vulnerabilidad de Seguridad en RealPlayer* y la *Actualización de Seguridad para RealPlayer*.

VI. Apéndice B. Referencias

- Soporte de usuario Actualizaciones de Seguridad de RealPlayer - <http://service.real.com/realplayer/security/191007_player/en/>
- Actualización de Seguridad para RealPlayer - <http://docs.real.com/docs/security/SecurityUpdate101907Player.pdf>
- Nota de Vulnerabilidad del US-CERT VU#871673 - <http://www.kb.cert.org/vuls/id/871673>
- Asegurando tu navegador Web - <http://www.us-cert.gov/reading_room/securing_browser/#Internet_Explorer>

El Departamento de Seguridad en Cómputo/UNAM-CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E-Mail: seguridad@seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 43