Subdirección de Seguridad de la Información - UNAM-CERT -- DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2010-022 Uso de Librerías Dinámicas inseguras en Microsoft Windows

Dado la forma en que Microsoft Windows carga librerías dinámicas (DLLs), una aplicación podría cargar una DLL creada por un atacante en lugar de una legítima, trayendo consigo una ejecución de código arbitrario.

- **Fecha de Liberación:** 26-Ago-2010
- **Ultima Revisión:** 26-Ago-2010
- **Fuente:** CERT/CC
- **CVE ID:** TA10-238A
- **Riesgo** Crítico
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

1. Sistemas Afectados

Cualquier aplicación corriendo en Microsoft Windows que haga uso de DLLs podría verse afectada. El que sea vulnerable o no la aplicación, depende de como carga de manera específica una DLL. En la nota VU#707943 se especifican algunos proveedores en específico.

2. Descripción

Microsoft Windows hace uso de Librerías dinámicas (DLLS) que se cargan cuando son requeridas por una aplicación. Las DLLs son llamadas por lo general, al iniciar alguna aplicación; aunque pueden cargarse y liberarse mientras la aplicación esta en ejecución. Una aplicación puede solicitar una DLL de diferentes maneras, y Windows usa diferenes algoritmos de búsqueda para encontrar los archivos correspondientes a dichas DLLs. La interacción entre la aplicación y Windows puede conlleva a ue la DLL se cargue del mismo directorio en el que se está ejecutando la aplicación, desde el directorio de sistema o bien, desde donde la aplicación e encuentra instalada.

El directorio desde donde se ejecuta la aplicación puede ser el Escritorio, un dispositivo removible como una USB, un directorio compartido en red, o desde un servicio de directorios WebDAV. Cuando se abre un archivo asociado a una aplicación, una DLL en el mismo directorio puede cargarse. A pesar de que un atacante puede no tener permisos para escribir en la carpeta de sistema o sobre los directorios de aplicación, éste podría crear una DLL en el directorio usado para guardar archivos o bien, especificar un directorio que el especifique.

Los ataques contra este tipo de vulnerabilidad se conocen como "Binary Planting".

Se puede encontrar mas información en la nota VU#707943 y Microsoft Security Advisory 2269637

3. Impacto

Sustituyendo una DLL con el nombre correcto (y posiblemente con la ruta relativa) en el directorio de trabajo, un atacante puede ejecutar código con los privilegios de la aplicación que carga el la DLL.

4. Solución

Las aplicaciones que se ejecutan en una plataforma Windows podrían requerir actualizaciones o parches de manera individual. El artículo de Microsoft Knowledge Base KB2264107 describe una actualización que genera una llave de registro que previene que Windows busque DLLs en el directorio de la aplicación.

La información para soluciones específicas de diferentes productos, técnicas de mitigación General, y métodos seguros para que las aplicaciones carguen DLLs pueden encontrarse en la sección de **Vendor Information and Solution** de la nota de vulnerabilidad VU#707943

5. Referencias

- Vulnerability Note VU#707943
- Microsoft Security Advisory 2269637
- A new CWDIllegalInDllSearch registry entry is available to control the DLL search path algorithm

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

- Manuel Ignacio Quintero Martínez (mquintero at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subsecretaria de Seguridad de la Información
incidentes at seguridad.unam.mx
phishing at 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 47