UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Nota de Seguridad UNAM−CERT−2009−001

Microsoft Windows no deshabilita la propiedad Autorun

Deshabilitar el Autorun en los sistemas operativos Windows podría prevenir la propagación de códigos maliciosos. De cualquier manera, las guías de Microsoft para deshabilitar el Autorun no son completamente efectivas, lo que podría considerarse como una vulnerabilidad.

Fecha de Liberación: 20 de Enero de 2009

Ultima Revisión: 20 de Enero de 2009

Fuente: US−CERT

Problema de Vulnerabilidad

Local y remoto

I. **Sistemas Afectados**

- Microsoft Windows

II. **Descripción**

Microsoft Windows incorpora la característica Autorun, la cual podría ejecutar código arbitrario de manera automática cuando se conecta un dispositivo externo. El Autorun (al igual que la característica AutoPlay) podría permitir inadvertidamente la ejecución remota de código bajo las siguientes circunstancias:

- Cuando se conecta un dispositivo externo. Esto podría incluir a dispositivos como CD o DVD, dispositivos USB o Firewire y también al mapear unidades de red, otros dispositivos también podrían ser considerados. La simple conexión de este tipo de dispositivos podría permitir la ejecución de código sin la interacción del usuario.
- Al dar clic sobre el dispositivo externo a través de Windows Explorer. Cuando los usuarios dan clic sobre el dispositivo para ver su contenido en lugar de explorarlo podrían ocasionar la ejecución de código.
- Cuando el usuario selecciona una opción del menú de diálogo AutoPlay que aparece cuando un dispositivo externo es conectado.

Software malicioso, como W32.Downadup, utiliza el Autorun para propagarse. Por lo que deshabilitar esta característica como se especifica en el blog de Análisis de Vulnerabilidades de CERT/CC, podría prevenir efectivamente la propagación de código

malicioso.

Los valores de registro Autorun y NoDriveTypeAutorun no son eficientes para deshabilitar las características del Autorun en los sistemas Microsoft Windows. Establecer el valor de registro Autorun a cero no prevendrá que cuando se conecten nuevos dispositivos se ejecute el código contenido en el archivo Autorun.inf de manera automática. Lo que se ocasionará es que se deshabiliten los mensajes de notificación (Media Change Notification), los cuales podrían prevenir a Windows la detección de que un CD o DVD ha sido cambiado. De acuerdo a Microsoft, establecer el valor de registro NoDriveTypeAutorun a 0xFF "deshabilita el Autoplay en todo tipo de dispositivos". Sin embargo, a pesar de que este valor esté establecido, Windows ejecutará código arbitrario cuando el usuario de clic en el ícono del dispositivo a través de Windows Explorer.

III. Impacto

Al colocar el archivo Autorun.inf en un dispositivo externo (como memorias USB, CDs, etc.), un atacante podría ejecutar código arbitrario de manera automática al conectar el dispositivo en un sistema Windows. La ejecución de código también puede ocurrir cuando el usuario intenta explorar el contenido del dispositivo a través de Windows Explorer.

IV. Solución

Para desactivar por completo el Autorun en Microsoft Windows, active la siguiente clave de registro:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf]

@="@SYS:DoesNotExist"
```

Para asignar dicho valor, realice lo siguiente:

1. Copie el texto anterior
2. Pegue el texto en el Bloc de Notas (Notepad)
3. Guarde el archivo como *autorun.reg*
4. Abra la carpeta donde guardó el archivo
5. De doble clic en el archivo para importarlo al registro de Windows

Microsoft podría almacenar en la caché información del Autorun de dispositivos previamente montados en el equipo a través de la clave de registro MountPoints2. Se recomienda reiniciar Windows después de haber realizado los cambios al registro reiniciar el sistema operativo para que cualquier información guardada en la caché sea reinicializada y así pueda ser ignorado el archivo Autorun.inf. Otra alternativa podría ser eliminar la siguiente clave de registro:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
```

Una vez que se han realizado dichos cambios, los escenarios de ejecución descritos anteriormente habrán sido mitigados debido a que Windows no analizará los archivos Autorun.inf para determinar qué acciones deberá realizar. Mayores detalles pueden encontrarse en el blog de Análisis de Vulnerabilidad de CERT/CC.

V. Referencias

- The Dangers of Windows AutoRun − http://www.cert.org/blogs/vuls/2008/04/the_dangers_of_windows_autorun.html
- Microsoft Windows Does Not Disable AutoRun Properly − http://www.us−cert.gov/cas/techalerts/TA09−020A.html

---

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

- Oscar Raúl Ortega Pacheco (oortega at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
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