UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−018

Buffer Overflow en el Manejo de Metarchivos en Microsoft Windows

---

Microsoft Windows es vulnerable a una ejecución remota de código a través de un error en el manejo de archivos utilizando el formato de imagen Metarchivo de Windows. El código de exploit ha sido liberado públicamente y utilizado para atacar satisfactoriamente sistemas Windows XP con SP2 completamente actualizados. Sin embargo, otras versiones del sistema operativo Windows podrían estar también en riesgo.

Fecha de Liberación:	28 de Diciembre de 2005
Ultima Revisión:	28 de Diciembre de 2005
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

Microsoft Windows todas las versiones	**Metarchivo de Windows**	<=KB896424

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Buffer Overflow

I. Descripción

Los Metarchivos de Microsoft Windows son archivos de imagen que pueden contener información de un vector o de una imágen basada en mapa de bits. Microsoft Windows contiene rutinas para desplegar varios formatos de Metarchivo de Windows. Sin embargo, una falla en la validación de entrada en una de estas rutinas podría permitir que ocurra un buffer overflow y podría permitir la ejecución remota de código arbitrario.

Esta nueva vulnerabilidad podría ser similar a la liberada por Microsoft en Boletín de Seguridad de Microsoft MS05−053. Sin embargo, el código de exploit disponible públicamente se sabe que afecta a sistemas actualizados con los parches del MS05−053.

No todos los productos antivirus son actualmente capaces de detectar todas las variantes de exploits conocidos para esta vulnerabilidad. Sin embargo. El US−CERT/UNAM−CERT recomienda actualizar todas las firmas antivirus para proporcionar una máxima protección como nuevas variantes aparezcan.

El US−CERT está dando seguimiento a esta vulnerabilidad como VU#181038. Éste número de referencia corresponde a la entrada CVE CVE−2005−4560

II. Impacto

Un intruso remoto no autenticado podría ser capaz de ejecutar código arbitrario si un usuario es persuadido a visualizar un Metarchivo de Windows creado de forma maliciosa.

III. Solución

Debido a que la fecha no existe ninguna actualización para éste problema, el US−CERT/UNAM−CERT recomienda a los sitios seguir varias soluciones temporales potenciales.

Soluciones temporales

Sea conciente que el US−CERT/UNAM−CERT ha confirmado que el filtrado basado solo en la extensión de archivo WMF o application/x−msMetafile tipo MIME no bloqueará todos los vectores de ataque conocidos para esta vulnerabilidad. Los mecanismos de filtrado deberían ser buscando cualquier archivo que Microsoft Windows reconozca como un Metarchivo de Windows en virtud de su encabezado de archivo.

No acceda a Metarchivos de Windows de fuentes no confiables

Los exploits ocurren accediendo a Metarchivos de Windows creados de forma maliciosa. Accediendo solamente a Metarchivos de Windows confiables o de fuentes conocidas, las oportunidades de explotación serán reducidas.

Los intrusos podrían almacenar Metarchivos de Windows maliciosos en un sitio Web. Con el propósito de convencer a los usuarios para que visiten el sitio Web, los intrusos a menudo utilizan URLs codificados, variaciones de direcciones IP, URLs largos, nombres mal escritos de forma intencional y otras

técnicas para crear vínculos Web maliciosos. No haga clic en hipervínculos no solicitados recibidos vía correo electrónico, mensajes instantáneos, foros Web o canales de Chat. Escriba directamente en el navegador para evitar estos hipervínculos maliciosos. Mientras estas son buenas prácticas de seguridad, siguiendo estos comportamientos no prevendrá la explotación de ésta vulnerabilidad en todos los casos, particularmente si un sitio confiable ha sido comprometido o permite cross−site scripting.

Bloquear el acceso a Metarchivos de Windows en el perímetro de la red

Bloqueando el acceso a Metarchivos de Windows utilizando proxies HTTP, gateways de correo electrónico, y otras tecnologías de filtrado de red, los administradores de sistemas también podrían limitar otros vectores de ataque potenciales.

Reiniciar los programas asociados para los Metarchivos de Windows

Remapeando el manejo de Metarchivos de Windows para abrir un programa diferente al predeterminado Windows Picture and Fax Viewer (SHIMGVW.DLL) podría prevenir la explotación a través de algunos vectores de ataque actuales. Sin embargo, esto podría aún permitir que la vulnerabilidad sea explotada a través de otros vectores de ataque conocidoss

---

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