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 75/ 31 de Octubre de 2008

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

CONTENIDO

FUENTES

- Hispasec
- Microsoft
- Winzip
- Info Security
- Xerox

VULNERABILIDAD EN CÓDIGO A TRAVÉS DE WINZIP EN WINDOWS 2000

Se han encontrado problemas de seguridad en WinZip 11.x que podrían ser aprovechadas para ejecutar código arbitrario en sistemas Windows 2000.

WinZip es unos de los compresores más extendidos debido a su modo sencillo de trabajar con los archivos y a que permite el manejo de numerosos formatos de compresión, siendo el .zip el usado por defecto.

Las vulnerabilidades encontradas están causadas porque WinZip 11.x incluía en la carpeta del programa una versión vulnerable de la librería GDI+ de Windows (gdiplus.dll) para procesar archivos de imagen. –La versión 11.0 la incluía siempre aunque las 11.1 y 11.2 sólo si los equipos estaban basados en Windows 2000.

Aprovechándose de esta circunstancia, un atacante remoto podría ejecutar código arbitrario si un usuario hiciera uso del modo de visualización para intentar acceder una imagen especialmente modificada contenida en un archivo zip.

La versión 12 de WinZip, que tampoco sería vulnerable, se puede obtener desde: http://update.winzip.com/downwz.htm

MÁS INFORMACIÓN:

- **WinZip 11.2 SR-1 (Build 8261)**
  http://update.winzip.com/wz112sr1.htm
- **Boletín de seguridad de Microsoft MS08-052**
  Vulnerabilidades en GDI+ podrían permitir la ejecución remota de código
  http://www.microsoft.com/spain/technet/security/bulletin/ms08-052.mspx
- **09/09/2008 Boletines de seguridad de Microsoft en septiembre**
  http://www.hispasec.com/unaaldia/3608

VULNERABILIDAD EN CÓDIGO EN IMPRESORAS MULTIFUNCIÓN XEROX

Se ha encontrado una vulnerabilidad en el controlador de red/ESS de las impresoras multifunción WorkCentre de Xerox que podría ser explotada por un atacante de la red local para ejecutar código arbitrario en la impresora.

La vulnerabilidad está causada por un desbordamiento de búfer en Samba al manejar respuestas SMB (Service Message Block) remotas.

Samba es una implementación Unix "Open Source" del protocolo SMB/NetBIOS, utilizada para la compartición de archivos e impresora en entornos Windows. Gracias a este programa, se puede lograr que máquinas Unix y Windows convivan amigablemente en una red local, compartiendo recursos comunes.

Si un atacante consigue tomar el control de una impresora podría cambiar la configuración de la misma; pero además podría conseguir cierta información sensible, ya que tendría acceso a la memoria del dispositivo donde residen aquellos documentos copiados o imprimidos recientemente.

La vulnerabilidad está confirmada para las siguientes versiones de impresoras multifunción:

Xerox WorkCentre: 232, 238, 245, 255, 265, 275, 7655, 7665, 7675, 5623, 5635, 5645, 5655, 5665, 5675 y 5687.

Xerox WorkCentre Pro: 232, 238, 245, 255, 265 y 275.

RECOMENDACIÓN :

El fabricante recomienda consultar la tabla de versiones vulnerables (disponible en el boletín de seguridad) y aplicar el parche P36v1, disponible para su descarga desde:

http://www.xerox.com/downloads/usa/en/c/cert_P36v1_WCP275_WC7675_WC5687_Patch.zip

MÁS INFORMACIÓN:

- **Xerox Security Bulletin XRX08-009: Software update to address Network Controller vulnerability**
  http://www.xerox.com/downloads/usa/en/c/cert_XRX08_009.pdf

ACTUALIZACIÓN DEL KERNEL PARA PRODUCTOS SUSE LINUX 10 SP1

SuSe ha publicado una actualización del kernel de Linux para productos SuSE Linux 10 SP1 que corrige múltiples vulnerabilidades que podrían permitir a un atacante local o remoto acceder a información sensible, saltarse restricciones de seguridad, causar una denegación de servicio o potencialmente ejecutar código arbitrario.

Los problemas corregidos son:

- Se ha corregido un fallo en el chequeo de privilegios de usuario de la función sbni_ioctl del driver SBNI que podría permitir a un usuario local elevar privilegios.
- Se ha corregido un fallo en el chequeo de privilegios de usuario en la función do_change_type de fs/namespace.c que podría permitir a un usuario local elevar privilegios o causar una denegación de servicio modificando las propiedades de los puntos de montaje.

MÁS INFORMACIÓN:

- **[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:2008:049)**
  http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00003.html

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106