

BOLETÍN DE SEGURIDAD DE XEROX - XRX08-001

Existen vulnerabilidades en el controlador de red/ESS que, si se aprovechan, podrían permitir a usuarios remotos no autorizados ejecutar una variedad de código a través de solicitudes de llamada de procedimientos remotos (del inglés RPC).

Para los productos indicados se proporciona la siguiente solución de software (parche P32) y las instrucciones de automantenimiento. Este parche está diseñado para que lo instale el cliente. La solución de software se encuentra comprimida en un archivo zip de 8.3 MB al que se puede acceder a través del enlace siguiente:

http://www.xerox.com/downloads/usa/en/c/cert_P32v2_WCP275_WC7665_Patch.zip

El parche P32 está considerado como parche **Importante**.

Los clientes preocupados por esta vulnerabilidad en los productos que se listan más abajo, primero deben usar las instrucciones de instalación adjuntas para verificar que disponen de una versión para la que se debe instalar el parche y, en el caso de que dispongan de una, deberán seguir las instrucciones de instalación para instalar el parche.

- Para los productos de la serie WorkCentre® / WorkCentre® Pro 2xx, la versión de software del sistema *.60.22.007 o superior (versión del controlador ESS 040.022.x1110 o superior) ya contiene esta solución, por lo que la instalación del parche no es necesaria.
- Para los productos de la serie WorkCentre® 7655/7665, la versión de software del sistema 040.032.55080 o superior (versión del controlador ESS 040.032.55080 o superior) ya contiene esta solución, por lo que la instalación del parche no es necesaria. Además, en el caso de un sistema WorkCentre® 7655/7665, si el software del sistema no tiene la versión 040.032.53080 o superior (versión del controlador de red 040.022.*1031 o superior), deberá ponerse en contacto con un técnico de servicio para actualizar la máquina con la versión de software del sistema/controlador de red 040.032.53080 para que pueda aplicarse el parche.

Nota: este parche de seguridad se ha designado como parche **P32**. Una vez que el parche se ha instalado correctamente, la versión del controlador de red mostrará **.P32** (Ej. 040.022.x0115.P32).

Antecedentes

Como parte de los continuos esfuerzos de Xerox por proteger a sus clientes, se han detectado las siguientes vulnerabilidades:

- CVE-2007-2446: múltiples desbordamientos de la pila permiten la ejecución remota de código
- CVE-2007-2447: vulnerabilidad de ingreso de comandos remotos

Estas vulnerabilidades en el código del controlador de red/ESS que manipula servicios de uso de compartido de impresora y archivos para clientes SMB (Service Message Block)/CIFS (Common Internet File System) tales como los dispositivos multifunción de Xerox, podrían permitir a usuarios remotos no autorizados a ejecutar una variedad de código a través de secuencias de solicitudes de llamadas de procedimientos remotos especialmente desarrolladas. Estas vulnerabilidades afectan solo a los servicios de uso compartido de la impresora. Si lo consigue, un usuario no autorizado podría realizar cambios en la configuración del sistema. Las claves de los usuarios y los clientes no están expuestas a este peligro.

Este parche afecta exclusivamente a las versiones de equipos conectados en red de los siguientes productos¹:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
7655	
7665	

¹Si el producto no se encuentra conectado en red, no es vulnerable y no requiere acción alguna.

Solución

Instrucciones de instalación

Nombre del archivo de parche: **WCP275_WC7665_P32v2.dlm**

Este parche puede instalarse en los sistemas tal como se indica a continuación.

Resumen de versiones y acciones:

- Determine la versión inicial del software del sistema o la versión del controlador ESS.
- Determine qué actualizaciones se necesitan.
- Actualice los dispositivos según se precise.
- Aplique el parche si es necesario.

Para WC/WCP 232/238/245/255/265/275

	Si su versión de software es SW sistema o Controlador ESS		¿Listo para el parche ?	Siguiente paso:	Después:	El controlador de red/ESS mostrará:
1	*.27.24.000 a *.27.24.020	040.010.#0930 a 040.010.#1160	No	Actualizar a *.60.22.000 o superior. Ver el apéndice A	Cargar el parche P32	040.022.#1031.BIOSxx.xx.P32 v2
2	*.50.03.000 a *.50.03.009	040.010.#1172 a 040.010.#2250	No	Actualizar a *.60.22.000 o superior. Ver el apéndice A	Cargar el parche P32	Si se aplica el parche, 040.022.#1031.BIOSxx.xx.P32 v2
3	*.50.03.011	040.010.#2280	No	Llamar al servicio técnico para actualizar a *.60.22.000 o superior	Cargar el parche P32	Si se aplica el parche, 040.022.#1031.BIOSxx.xx.P32 v2
4	*.27.24.015 con certificación Common Criteria	040.010.#1121	No	Ver NOTA 1, más abajo	-	-
5	*.39.24.001 con certificación Common Criteria	040.010.#1123	No	Ver NOTA 1, más abajo	-	-
6	*.60.15.000	040.022.#0112	No	Actualizar a *.60.22.000 o superior Ver el apéndice A	Cargar el parche P32	040.022.#1031.BIOSxx.xx.P32 v2
7	*.60.17.000 con certificación Common Criteria	040.022.#0115	Sí	Ver NOTA 1, más abajo	-	Si se aplica el parche, 040.022.#0115.P32v2
8	*.60.17.000 a *.60.22.006	040.022.#0115 a 040.022.#1100	Sí	Cargar el parche P32	-	040.022.#0115.BIOSxx.xx.P32 v2 a 040.022.#1100.BIOSxx.xx.P32 v2
9	*.60.22.007 y superior	040.022.#1110 o superior	N/A	Completado	-	-

NOTA 1: si el dispositivo tiene una versión de software del sistema *.27.24.015, *.39.24.001 o *.60.17.000, su dispositivo está en una configuración de certificación Common Criteria (criterios comunes). Si aún no está en *.60.17.000, podrá actualizar a *.60.17.000 y después cargar el parche P32, pero el dispositivo no estará más en una configuración de certificación Common Criteria.

Para WC 7655/7665

	Si su versión de software es SW sistema o Controlador de red		¿Listo para el parche?	Siguiente paso:	Después:	El controlador de red/ESS mostrará:
1	040.032.50855 a 040.032.51040	040.032.50855 a 040.032.51030	No	Llamar al servicio técnico para actualizar a 040.032.53080	Cargar el parche P32	040.032.53080.BIOSxx.xx.P32 v2
2	040.032.53080	040.032.53080	Sí	Cargar el parche P32	-	040.032.53080.BIOSxx.xx.P32 v2
3	040.032.53080 con certificación Common Criteria	040.032.53080	Sí	Ver NOTA 1, más abajo	-	Si se aplica el parche, 040.032.53080.BIOSxx.xx.P32 v2
4	040.032.55030 a 040.032.55070	040.032.55030 a 040.032.55070	Sí	Ver NOTA 1, más abajo	-	Si se aplica el parche, de 040.032.55030.BIOSxx.xx.P32 v2 a 040.032.55070.BIOSxx.xx.P32 v2
5	040.032.55080 y superior	040.032.55080	N/A	Completado	-	-

NOTA 1: si el dispositivo tiene una versión de software del sistema de 040.032.53080, el dispositivo está en una configuración de certificación Common Criteria (criterios comunes). Puede cargar el parche P32 si lo desea, aunque el dispositivo dejará de estar en la configuración de certificación Common Criteria.

Instalación del parche

Es necesario descargar el parche. El parche está empaquetado en formato ZIP. Descargue el archivo ZIP de la dirección URL indicada y extraiga todo el contenido al escritorio. No intente abrir el archivo que tiene la extensión .DLM. Este es el parche y se debe cargar en el producto multifunción.

Métodos de instalación del parche

Este parche y la actualización (como la mayoría del software) puede y debe instalarlo el cliente. Existen varios métodos.

- Enviar un archivo de parche/actualización al dispositivo a través de la página web del mismo (método de actualización del software de la máquina).
- Actualizar/instalar el parche en un solo dispositivo mediante un comando LPR.
- Actualizar/instalar el parche en varios dispositivos mediante un lote de comandos LPR.
- Utilizar el servicio web de CentreWare y XDM para enviar archivos de parches/actualizaciones a varios dispositivos.

Para obtener información adicional sobre los métodos descritos, consulte el consejo para el cliente "How to Upgrade, Patch or Clone Xerox Multifunction Devices" (cómo actualizar, instalar un parche o clonar dispositivos multifunción Xerox) en <http://www.office.xerox.com/support/dctips/dc06cc0410.pdf>.

Método de actualización del software de la máquina

- 1) Abra un navegador web y conéctese al dispositivo multifunción. Para ello, introduzca el número de IP del dispositivo.
- 2) Seleccione el icono "Índice" situado en la parte intermedia superior de la pantalla.
- 3) Seleccione "Software de la máquina (Actualizaciones)".
- 4) Introduzca el nombre de usuario y la clave del dispositivo.
- 5) En la sección "Actualización manual", seleccione el botón Examinar para buscar y seleccionar el archivo **WCP275_WC7665_P32v2.dlm**.
- 6) Haga clic en el botón "Instalar software".
- 7) Todos los WCP imprimirán una hoja de instalación del parche y se reiniciarán automáticamente para instalar el parche. El parche se instala cuando se añade **.P32v2** al número de versión del controlador de red (ESS).

Apéndice A - Obtención del software del sistema

Para obtener la versión de software del sistema *.60.22.000 o posterior:

- a) Utilice un navegador para ir a www.xerox.com.
- b) Seleccione el enlace "Asistencia y controladores".
- c) Seleccione "Multifuncionales".
- d) Seleccione "WorkCentre" o "WorkCentre Pro", según el producto que posea.
- e) Localice el enlace correspondiente al modelo de WorkCentre.
- f) Seleccione "Controladores y descargas".
- g) Seleccione el enlace de "Actualización del equipo".
- h) Seleccione el enlace de "System software set *.60.22.000 install instructions" e imprima o guarde las instrucciones.
- i) Seleccione el enlace de "System Software set *.60.22.000" y guarde el archivo en el PC.
- j) Una vez descargado, extraiga los archivos al escritorio.
- k) Revise las instrucciones de instalación del software del sistema que había guardado.
- l) Actualice el dispositivo.

Apéndice B: Activación de LPD, impresión a través del puerto 515

Para utilizar el método LPR para enviar el parche, el dispositivo multifunción debe admitir la función LPD (Line Printer Daemon) a través del puerto 515. La mayoría de los dispositivos multifunción tienen activada esta función de manera predeterminada. Si ha desactivado la impresión LPD, debe volver a activarla para utilizar el método LPR.

Siga estos pasos para activar LPD:

- 1) Abra un navegador web y conéctese al dispositivo multifunción. Para ello, introduzca el número de IP del dispositivo.
- 2) Seleccione el icono "Índice" o "Índice de dispositivo" situado en la parte superior de la pantalla.
- 3) Seleccione "LPR/LPD" o "LPD".
- 4) Si la casilla Activado NO está marcada, añada una marca de verificación.
- 5) Seleccione "Aplicar opciones nuevas".
- 6) Introduzca el nombre de usuario y la clave del administrador y luego seleccione Aceptar.
- 7) Reinicie el dispositivo multifunción desde la página web Estado o con el botón de desconexión del dispositivo.

Exención de responsabilidad

La información incluida en este documento se proporciona "tal cual", sin garantía de ningún tipo. Xerox Corporation deniega cualquier garantía, ya sea explícita o implícita, incluyendo las garantías de comerciabilidad y adecuación para un fin en particular. En ningún caso Xerox Corporation será responsable de ningún daño que se derive del uso o la falta de uso que haga el usuario de la información que se proporciona en este documento, que incluye, sin limitación, daños indirectos, incidentales, consecuentes, pérdida de beneficios comerciales o daños especiales, aunque Xerox Corporation hubiese sido advertida de la posibilidad de que se produjeran dichos daños. Algunos estados no permiten la exclusión o limitación de responsabilidad por daños consecuentes, de manera que estas limitaciones pueden no aplicarse.