

## **BOLETÍN DE SEGURIDAD DE XEROX XRX05-006**

La vulnerabilidad en el servidor web MicroServer de Xerox podría permitir el acceso no autorizado.

La siguiente solución de software y las instrucciones de automantenimiento que se proporcionan para los productos indicados sirven para proteger los datos confidenciales de posibles ataques a través de la red.

La solución de software está comprimida en un archivo zip de 581 KB. Puede acceder a ella a través del enlace de este boletín en Xerox.com / Seguridad:

[http://www.xerox.com/downloads/usa/en/c/cert\\_P22\\_NIAP\\_WCP\\_C\\_Only.zip](http://www.xerox.com/downloads/usa/en/c/cert_P22_NIAP_WCP_C_Only.zip)

### **Antecedentes**

La vulnerabilidad del código del servidor web podría permitir el acceso no autorizado a la estructura de directorios del servidor:

- Se podría pasar por alto la autenticación.
- Las solicitudes del HTTP construido especialmente podrían causar una denegación de servicio o permitir el acceso no autorizado en una máquina atacada.
- Creación de secuencias de comandos entre sitios que permiten modificar el contenido de las páginas web sin autorización.

Si lo consigue, un atacante podría realizar cambios no autorizados en la configuración del sistema. Las claves de los usuarios y los clientes no están expuestas a este peligro.

**Nota: el software del parche sólo se debe aplicar a los siguientes productos.**

### **Productos afectados:**

#### **WorkCentre® Pro**

C2128

C2636

C3545

## Solución

### Parche para el servidor web MicroServer Edición: 21/06/05

Hay disponible un parche que soluciona el problema de vulnerabilidad en el servidor web MicroServer de Xerox que se ha identificado en los dispositivos multifunción (MDF) WorkCentre C2128/2636/3545. Solo se debe aplicar el software del parche al MFD si la versión del software del sistema del MFD es una de las que se indican.

Es necesario descargar el parche. El parche está empaquetado en formato ZIP. Descargue el archivo ZIP de la URL indicada y extraiga todo el contenido al escritorio. **NO INTENTE ABRIR EL ARCHIVO CON LA EXTENSIÓN .TGZ.** Es el parche y se ha de cargar en el MFD tal cual.

### Instrucciones de instalación

Nombre del archivo del parche: **P22\_niap\_wcp\_c.tgz**

Este parche solo es necesario si WorkCentre dispone de una de las siguientes versiones del software del sistema:

**WorkCentre Pro Color 2128/2636/3545 de la versión 0.001.04.044 a la 0.001.04.505**

**Si su dispositivo dispone de una versión superior del software del sistema, no necesita instalar el parche.**

#### **Confirme la versión del software del sistema.**

Para determinar la versión del software del sistema, imprima un informe de configuración o consulte la versión en la interfaz del cliente web.

Para imprimir un informe de configuración desde la interfaz de usuario local en la máquina:

- 1) Pulse el botón Estado de máquina.
- 2) Seleccione Imprimir informe de configuración.
- 3) Busque el número de la versión del software del sistema.

Para ver la versión desde la interfaz del cliente web:

- 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 "Configuración".
- 4) Desplácese a "Configuración de la impresora", ubicación que muestra la versión del software del sistema.

#### **Instale el parche**

**NO INTENTE ABRIR EL PARCHE, YA QUE PODRÍA DAÑAR EL ARCHIVO.**

Hay dos formas de cargar el parche para este modelo.

- 1) Método LPR
- 2) Método de actualización del software de la máquina

#### **Método LPR desde un equipo Windows NT, 2000 o XP**

Para este método, es necesario activar el protocolo LPR en el dispositivo. Compruebe en el informe de configuración si el protocolo está activado. Este protocolo se puede activar por medio de la interfaz de usuario local o de la interfaz web. Consulte las instrucciones del Apéndice A.

- 1) Abra un indicativo de comandos en MS DOS. Para ello, seleccione el icono "Inicio" de Windows y, a continuación, "Ejecutar". Escriba "cmd" y seleccione <Intro>.
- 2) Envíe el archivo del parche mediante la línea de comandos: **lpr -S <printer\_ip> -Pip  
P22\_NIAP\_WCP\_C Only.tgz**

- 3) WorkCentre se reiniciará automáticamente para instalar el parche.
- 4) El parche estará instalado cuando se haya añadido **.P22** al número de versión del controlador de red.

## 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 del usuario, Admin y la clave del administrador del dispositivo.
- 5) En la sección "Actualización manual" haga clic en el botón Examinar para buscar y seleccionar el archivo **P22\_NIAP\_WCP\_C Only.tgz**
- 6) Haga clic en el botón "Instalar software".
- 7) WorkCentre se reiniciará automáticamente para instalar el parche.
- 8) El parche estará instalado cuando se haya añadido **.P22** al número de versión del controlador de red.

## Exclusión de responsabilidad

La información incluida en esta respuesta de producto Xerox se proporciona "tal cual", sin ninguna garantía de ningún tipo. Xerox Corporation deniega cualquier garantía, ya sea explícita o implícita, incluyendo las garantías de comerciabilidad y adecuación a 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 esta respuesta de producto de Xerox, lo que incluye 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. En algunos estados, no se permite la exoneración o la limitación de la responsabilidad para los daños consecuentes, por lo que es posible que la limitación anterior no sea aplicable en su caso.