XEROX SECURITY BULLETIN XRX04-007

Vulnerability in the Xerox MicroServer Web Server could cause a denial of service.

The following software solution and self-service instructions are provided for the listed products to protect your confidential data from possible attacks through the web.

The software solution is compressed into a 2.3 MB zip file and can be accessed in the link following this bulletin on:

http://www.xerox.com/downloads/usa/en/c/cert_XRX04D_patch.zip

Background

There is memory corruption vulnerability in the web server code that could cause a denial of service to an attacked machine. The vulnerability can be exploited using a specially constructed URL to navigate through the directory. An attacker could use this URL to force the web server to restart. Theoretically an attacker could continually disable an entire network of machines on purpose by submitting the appropriate URL to the web server on each machine on a continual basis (e.g., by using a properly crafted URL), causing the machines to constantly be rebooted.

Products Affected:

WorkCentre®	WorkCentre® Pro
M35	32 Color
M45	35
M55	40 Color
	45
	55

Solution

HTTP Memory Patch Install Process

Edited: 30-Aug -2004

There is a patch available that fixes an HTTP memory issue identified on WorkCentre Multifunction Devices (MFD). The patch software only needs to be applied to the MFD if the Network Controller software version of your MFD falls within the range listed.

You must download the patch. The patch is packaged in a ZIP format. Download the ZIP file from the URL provided and extract all contents to your desktop. DO NOT TRY TO OPEN THE FILE WITH THE .TGZ EXTENSION. This is the patch and must be loaded on the MFD as is.

Instructions for the WorkCentre + PS M35/M45/M55, WorkCentre Pro 35/45/55, and the WorkCentre Pro 32/40 Color.

This patch is only needed if your WorkCentre falls within the following Net Controller versions:

WorkCentre + PS M35/M45/M55, WorkCentre Pro 35/45/55, from 1.01.108.1 through 1.02.372.1

WorkCentre 32/40 Color, from 01.00.060 through 01.02.072.1

If your device has a higher Net Controller version, then you do not need to install the patch.

Confirm your Net Controller Software Version

To determine your Network Controller version, you can either print a Configuration Report or view the version on the Web client interface.

To print a configuration report from the local User Interface at the machine:

1) Press the Machine Status button
2) Select Print Configuration Report
3) Look for the Net Controller Software Version number

To view the version from the web client interface:

1) Open a web browser and connect to the multifunction device by entering the IP number of the device
2) Select the “Index” icon in the upper right corner
3) Select “Configuration”.
4) Scroll to the location that displays the Net Controller Software Version.

Install the Patch

DO NOT TRY TO OPEN THE PATCH AS IT MAY DAMAGE THE FILE.

This patch can be submitted one of two ways for this model.

1) LPR Method
2) Machine Software (Upgrade) Method

LPR Method from a Windows NT, 2000, or XP

This method requires that LPR Protocol be enabled on the device. Check the configuration report to see if the protocol is enabled. This protocol can be enabled via the Local User Interface or via the Web Interface. See Appendix A for instructions.

1) Open a “DOS Command Prompt”. You can do this by selecting the Windows “Start” icon, and selecting “Run”. Enter “cmd” and hit <Enter>.
2) Submit the patch file via the command line: **lpr –S <printer_ip> –P lp HTTP Memory P10-WCPAll.tgz**
3) The WorkCentre will automatically reboot in order to install the patch.
4) The patch is installed when **.P10** is appended to the Network Controller version number. The WorkCentre + PS M35/M45/M55 will NOT display **P10**, but the patch is installed.

Machine Software (Upgrade) Method

1) Open a web browser and connect to the multifunction device by entering the IP number of the device.
2) Select the “Index” icon in the upper right corner.
3) Select “Machine Software (Upgrades)”.
4) Enter the User Name, Admin, and the Admin Password of the device.
5) Under “Manual Upgrade” select Browse button to find and select the file, **HTTP Memory P10-WCPAll.tgz**.
6) Select the “Install Software” button.
7) The WorkCentre will automatically reboot in order to install the patch.
8) The patch is installed when **.P10** is appended to the Network Controller version number. The WorkCentre M35/M45/M55 + PS will NOT display **P10**, but the patch is installed.

Appendix A – Enabling LPD, port 515 printing

In order to use the LPR method to submit the patch, your MFD must support Line Printer Daemon (LPD) over port 515. Most MFD’s have this enabled by default. If you have disabled LPD printing, you must enable it to use the LPR method.
Use the following steps to enable LPD:

1) Open a web browser and connect to the multifunction device by entering the IP number of the device
2) Select “Index” icon in the upper right corner
3) Select “LPR/LPD” or “Line Printer Daemon”
4) If the Enabled box is NOT checked, select the box to add a check mark.
5) Select “Apply New Settings”
6) Enter the user name, Admin, and the admin password, then select OK.
7) Reboot the MFD either from the Status web page or by pressing the Power Off button at the MFD.

Disclaimer

The information provided in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply