XEROX SECURITY BULLETIN XRX08-001

Vulnerabilities exist in the ESS/ Network Controller that, if exploited, could allow remote attackers to execute arbitrary code via specially crafted Remote Procedure Call (RPC) requests.

The following software solution (patch P32) and self-service instructions are provided for the listed products. This patch is designed to be installed by the customer. The software solution is compressed into a 8.3 MB zip file and can be accessed via the link below:

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

The P32 patch is classified as an **Important** patch.

Customers concerned about this vulnerability in the products listed below should first use the attached installation instructions to verify that they have a release for which the patch should be installed and, if they do, then follow the installation instructions to install the patch.

- For WorkCentre®/ WorkCentre® Pro 2xx Series products, System Software Version *.60.22.007 or higher (ESS Controller Version 040.022.x1110 or higher) already contains this fix and the installation of the patch is not required.
- For WorkCentre® 7655/7665 products, System Software Version 040.032.55080 or higher (ESS Controller Version 040.032.55080 or higher) already contains this fix and the installation of the patch is not required. In addition, for a WorkCentre® 7655/7665 if the System Software is not 040.032.53080 or above (Net Controller Version 040.022.*1031 or above), a service rep must be contacted to upgrade the machine to System Software/Net Controller Version 040.032.53080, before the patch can be applied.

Note: This security patch is designated as patch **P32**. Once this patch is successfully installed, the Network Controller version will display **.P32** (Ex. 040.022.x0115.P32).

Background

As part of Xerox's on-going efforts to protect customers the following vulnerabilities were discovered:

- CVE-2007-2446 - Multiple Heap Overflows Allow Remote Code Execution
- CVE-2007-2447 - Remote Command Injection Vulnerability

These vulnerabilities in the ESS/ Network Controller code that handles file and printer sharing services for Service Message Block (SMB)/ Common Internet File System (CIFS) clients such as Xerox MFD devices, could allow remote attackers to execute arbitrary code via specially crafted Remote Procedure Call (RPC) requests. These vulnerabilities affect only the printer sharing services. If successful, an attacker could make unauthorized changes to the system configuration. Customer and user passwords are not exposed.

This Patch Applies To Network-Connected Versions[1] only of the following products:

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

[1] If the product is not connected to the network, it is not vulnerable and therefore no action is required.

Solution

Install Instructions

Patch file name: **WCP275_WC7665_P32v2.dlm**

This patch can be installed to your systems as outlined below.

Summary of versions and actions:

- Determine starting System Software version or ESS Controller Version
- Determine what upgrades are necessary
- Upgrade devices as needed
- Apply the patch if needed

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

	If Your Software Version Is System SW	or ESS Controller	Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	*.27.24.000 to *.27.24.020	040.010.#0930 to 040.010.#1160	No	Upgrade to *.60.22.000 or higher. See Appendix A	Load P32 patch	040.022.#1031.BIOSxx.xx.P32v2
2	*.50.03.000 to *.50.03.009	040.010.#1172 to 040.010.#2250	No	Upgrade to *.60.22.000 or higher. See Appendix A	Load P32 patch	If patch is applied 040.022.#1031.BIOSxx.xx.P32v2
3	*.50.03.011	040.010.#2280	No	Call Service to upgrade to *.60.22.000 or higher	Load P32 patch	If patch is applied 040.022.#1031.BIOSxx.xx.P32v2
4	*.27.24.015 Common Criteria Certified	040.010.#1121	No	See NOTE 1 below	-	-
5	*.39.24.001 Common Criteria Certified	040.010.#1123	No	See NOTE 1 below	-	-
6	*.60.15.000	040.022.#0112	No	Upgrade to *.60.22.000 or higher See Appendix A	Load P32 patch	040.022.#1031.BIOSxx.xx.P32v2
7	*.60.17.000 Common Criteria Certified	040.022.#0115	Yes	See NOTE 1 below	-	If patch is applied, 040.022.#0115.P32v2
8	*.60.17.000 to *.60.22.006	040.022.#0115 to 040.022.#1100	Yes	Load P32 patch	-	040.022.#0115.BIOSxx.xx.P32v2 to 040.022.#1100.BIOSxx.xx.P32v2 .
9	*.60.22.007 and above	040.022.#1110 or above	N/A	Done	-	-

NOTE 1: If your device has a System Software version of *.27.24.015, *.39.24.001, or *.60.17.000, then your device is in a Common Criteria certified configuration. If you are not already at that *.60.17.000, you can upgrade to *.60.17.000 and then load the P32 patch, although the device would then no longer be in a Common Criteria certified configuration.

For WC 7655/7665

	If Your Software Version Is System SW	or Net Controller	Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	040.032.50855 to 040.032.51040	040.032.50855 to 040.032.51030	No	Call Service to Upgrade to 040.032.53080	Load P32 patch	040.032.53080.BIOSxx.xx.P32v2
2	040.032.53080	040.032.53080	Yes	Load P32 patch	-	040.032.53080.BIOSxx.xx.P32v2
3	040.032.53080 Common Criteria Certified	040.032.53080	Yes	See NOTE 1 below	-	If patch is applied, 040.032.53080.BIOSxx.xx.P32v2
4	040.032.55030 to 040.032.55070	040.032.55030 to 040.032.55070	Yes	See NOTE 1 below	-	If patch is applied, 040.032.55030.BIOSxx.xx.P32v2 to 040.032.55070.BIOSxx.xx.P32v2
5	040.032.55080 and above	040.032.55080	N/A	Done	-	-

NOTE 1: If your device has a System Software version of 040.032.53080, then your device is in a Common Criteria certified configuration. You can load the P32 patch, although the device would then no longer be in a Common Criteria certified configuration.

Install the Patch

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 .DLM extension. This is the patch and must be loaded on the MFD as is.

Patch Installation Methods

This patch and upgrade (like most software) can and should be installed by the customer. There are a variety of methods available for this.

- Send an Upgrade / Patch file to the device using the device web page for Machine Software Upgrade method.
- Upgrade / Patch a single device using an LPR command.
- Upgrade / Patch several devices using a batch of LPR commands.
- Using XDM and CenterWare Web to send Upgrade / Patch files to several devices.

For additional information on the above methods refer to Customer Tip “How to Upgrade, Patch or Clone Xerox Multifunction Devices“ (http://www.office.xerox.com/support/dctips/dc06cc0410.pdf)

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 middle portion of the screen.
3) Select “Machine Software (Upgrades)”.
4) Enter the User Name and Password of the device.
5) Under “Manual Upgrade” select Browse button to find and select the file, **WCP275_WC7665_P32v2.dlm**.
6) Select the “Install Software” button.
7) All WCP’s will print a patch install sheet and automatically reboot in order to install the patch. The patch is installed when **.P32v2** is appended to the Network Controller (ESS) version number.

Appendix A - Obtaining System Software

To obtain system software versions *.60.22.000 or later:

a) Use a browser to navigate to www.xerox.com.
b) Select the link called “Support & Drivers”.
c) Select “Multifunction”.
d) Select “WorkCentre” or “WorkCentre Pro” depending on your model.
e) Locate the link for your WorkCentre model.
f) Select “Drivers & Downloads”.
g) Select the link for “Firmware & Machine Upgrades”.
h) Select the link for “System software set *.60.22.000 install instructions” and print or save these instructions.
i) Select the link for “System Software set *.60.22.000” and save the file to your computer.
j) Once downloaded, extract the files to your desktop.
k) Review the “System Software Install Instructions” that you saved.
l) Upgrade the device.

Appendix B – 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” or “Device Index” icon in the upper portion of the screen.
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