

# Xerox Security Bulletin XRX08-009

## Software update to address Network Controller vulnerability

v1.2  
10/16/08

### Background

A vulnerability exists in the ESS/ Network Controller that, if exploited, could allow remote attackers to execute arbitrary code via specially crafted Remote Service Message Block (SMB) responses. This could occur with buffer overflows and un-validated user input in the Samba third-party code that handles file and printer sharing services for SMB clients (including Xerox MFD devices). If successful, an attacker could make unauthorized changes to the system configuration; however, customer and user passwords are not exposed. This vulnerability affects only the printer sharing services.

As part of Xerox's on-going efforts to protect customers, a software solution is provided for the products listed below. This solution is designed to be installed by the customer. Please follow the procedures below to install the solutions to protect your product from possible attack through the network.

The software solution is compressed into a 2.3 MB zip file and can be accessed via the link below or via the link following this bulletin on [www.xerox.com /security](http://www.xerox.com/security). (Note: The ReadMe file included in this zip file provides the applicable license information for this patch)

[http://www.xerox.com/downloads/usa/en/c/cert\\_P36v2\\_WCP275\\_WC7675\\_WC5687\\_Patch.zip](http://www.xerox.com/downloads/usa/en/c/cert_P36v2_WCP275_WC7675_WC5687_Patch.zip)

This solution 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 \*.60.22.016 or higher (ESS Controller Version 040.022.\*1180 or higher) already contains this fix and the installation of the patch is not required.
- For WorkCentre® 7655/7665/7675 products, System Software Version 040.033.53050 or higher (ESS Controller Version 040.033.53050 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 040.032.\*\*\*\*\* (except for System Version 040.032.53080 – See Note 2 in the Installation Instructions) or above (Net Controller Version 040.032.\*\*\*\*\* or above), a service rep must be contacted to upgrade the machine to System Software/Net Controller Version 040.033.52800 before the patch can be applied.
- For WorkCentre® 56xx Series products, System Software Version 21.113.02.015 (ESS Controller Version 050.060.50920) already contains this fix and the installation of the patch is not required.

### Notes:

1. This security patch is designated as patch **P36v2**. Once this patch is successfully installed, the Network Controller version will display **.P36v2** (Ex. 040.022.x1031.BIOS07.07.P36v2).



This software solution applies to network-connected versions<sup>1</sup> of the following products:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
7655	
7665	
7675	
5632	
5638	
5645	
5655	
5665	
5675	
5687	

---

<sup>1</sup>If the product is not connected to the network, it is not vulnerable and therefore no action is required.

## Patch Install Process

### Edited: 10/06/08

#### Install Instructions

Patch file name: WCP275\_WC7675\_WC5687\_P36v2.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 P36 patch	040.022.#1031.BIOSxx.xx.P36v2
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 P36 patch	If patch is applied 040.022.#1031.BIOSxx.xx.P36v2
3	*.50.03.011	040.010.#2280	No	Call Service to upgrade to *.60.22.000 or higher	Load P36 patch	If patch is applied 040.022.#1031.BIOSxx.xx.P36v2
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 P36 patch	040.022.#1031.BIOSxx.xx.P36v2
7	*.60.17.000 Common Criteria Certified	040.022.#0115	No	See NOTE 1 below	-	If patch is applied, 040.022.#0115.P36v2
8	*.60.17.000 to *.60.18.000	040.022.#0115 to 040.022.#1031	No	Upgrade to *.60.22.000 or higher See Appendix A	Load P36 patch	040.022.#1031.BIOSxx.xx.P36v2
9	*.60.22.000 to *.60.22.015	040.022.#1031 to 040.022.#1170	Yes	Load P36 patch	-	040.022.#1031.BIOSxx.xx.P36v2 to 040.022.#1170.BIOSxx.xx.P36v2
10	*.60.22.016 and above	040.022.#1180 or above	N/A – fix already in	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. You can upgrade to \*.60.22.000 and then load the P36 patch, although the device would then no longer be in a Common Criteria certified configuration.

**For WC 7655/7665/7675**

	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.xxxxx	040.032.xxxxx	No	Call Service to Upgrade to 040.033.52800	Load P36 patch	040.033.52800.BIOSxx.xx.P36v2
2	040.032.53080 Common Criteria Certified	040.032.53080	No	See NOTE 2 below	-	If patch is applied, 040.033.52800.BIOSxx.xx.P36v2
3	040.033.50500 to 040.033.51010	040.033.50500 to 040.033.51010	Yes	Load P36 patch	-	040.033.50500.BIOSxx.xx.P36v2 to 040.033.51010. BIOSxx.xx.P36v2
4	040.033.52800 to 040.033.53040	040.033.52800 to 040.033.53040	Yes	Load P36 patch	-	040.033.52800.BIOSxx.xx.P36v2 to 040.033.53040.BIOSxx.xx.P36v2
5	040.033.53050 and above	040.033.53050	N/A – fix already in	Done	-	-

**NOTE 2:** If your device has a System Software version of 040.032.53080, then your device is in a Common Criteria certified configuration. You can call Xerox Service to upgrade the device to 040.033.52800 and then load the P36 patch, although the device would then no longer be in a Common Criteria certified configuration.

**For WC 5632/5638/5645/5655/5665/5675/5687**

	If Your Software Version Is System SW or Net Controller		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	21.113.02.000 Soon to be Common Criteria Certified	050.060.50812	Yes	See NOTE 3 below	-	050.060.50812. BIOSxx.xx.P36v2
2	21.105.01.000	050.060.50730	No	Upgrade to 21.113.02.000 or higher. See Appendix A	Load P36 patch	050.060.50812.BIOSxx.xx.P36v2
3	21.113.02.000 to 21.113.02.014	050.060.50812 to 050.060.50911	Yes	Load P36 patch	-	050.060.50812.BIOSxx.xx.P36v2 to 050.060.50911. BIOSxx.xx.P36v2
4	21.113.02.015	050.060.50920	N/A – fix already in	-	-	-

**NOTE 3:** Software Version 21.113.02.000 is soon to be Common Criteria Certified. Once certified, you can load the P36 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\_WC7675\_WC5687\_P36v2.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 **.P36v2** is appended to the Network Controller (ESS) version number.

### **Appendix A - Obtaining System Software**

**To obtain system software versions \*.60.22.000 or later for the WC/WCP2xx:**

- a) Use a browser to navigate to [www.xerox.com](http://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.

**To obtain system software versions 21.113.02.000 or later for WC56xx:**

- a) Use a browser to navigate to [www.xerox.com](http://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 21.113.02.000 install instructions” and print or save these instructions.
- i) Select the link for “System Software set 21.113.02.000 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

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.