Xerox Security Bulletin XRX08-004

Software update to address cross site scripting vulnerability

v1.0
05/22/08

Background

A persistent cross site scripting vulnerability exists in the Web Server of the products listed below. If exploited this vulnerability could allow code injection by malicious web users into the web pages viewed by other users. Customer and user passwords are not exposed.

This vulnerability was reported to us privately by Louhi Networks of Finland. Other than the proof-of-concept exploit code provided by the security researcher, Xerox is not aware of exploit code existing in the wild.

As part of Xerox's on-going efforts to protect customers, executable[1] or binary files containing the network controller software releases addressing this vulnerability are provided for the products listed below. These solutions are 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 solutions are compressed into one of six executable files depending on the desired product and can be accessed via the links below or via the links following this bulletin on http://www.xerox.com/security:

- WorkCentre 7132 Standard Executable -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-STD_EXEC.zip
- WorkCentre 7132 Standard Binary -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-STD_BIN.zip
- WorkCentre 7132 with Postscript Executable -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-PS_EXEC.zip
- WorkCentre 7132 with Postscript Binary -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-PS_BIN.zip
- WorkCentre 7228/7235/7245 Executable -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7228-7235-7245_EXEC.zip
- WorkCentre 7228/7235/7245 Binary -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7228-7235-7245_BIN.zip

These solutions are classified as a **Critical** patch.

Acknowledgment

Xerox wishes to thank Henri Lindberg, Louhi Networks, Finland (www.louhi.fi) for initially notifying us of this vulnerability.

This software solution applies to network-connected versions[2] of the following products:

WorkCentre®
7132
7228
7235
7245

[1] Firmware Update Tool for Windows – a firmware upgrade utility bundled with the software release that enables customer installation of the software release

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

Solution

Patch Install Process
Edited: 05/19/08

Install Instructions

Patch file name for WC 7228/7235/7245:

- cert_P35_WC7228_7235_7245_EXEC.zip (self-extracting executable)
- cert_P35_WC7228_7235_7245_BIN.zip (binary file to be used with Centreware Web)

Patch file name for WC 7132:

- cert_P35_WC7132-STD_EXEC.zip (STD version of self-extracting executable)
- cert_P35_WC7132-STD_BIN.zip (STD version of binary file to be used with Centreware Web)
- cert_P35_WC7132-PS_EXEC.zip (PS version of self-extracting executable)
- cert_P35_WC7132-PS_BIN.zip (PS version of binary file to be used with Centreware Web)

For WC 7132 PS version use cert_P35_WC7132-PS_EXEC.zip or cert_P35_WC7132-PS_BIN.zip
For WC 7132 STD Version use cert_P35_WC7132-STD_EXEC.zip or cert_P35_WC7132-STD_BIN.zip

	If Your Software Version Is Controller ROM	Ready for Patch?	Next step:	Then:	Controller ROM Will Now Show:
1	1.202.1 to below 1.202.6	Yes	Load patch (See Notes 1 and 2 for WC 7132 below)	-	1.202.6

NOTE 1 for WC 7132: For the WC 7132, it must first be determined which file to load on the device. The WC 7132 can be configured as a PS version or a STD version. To determine this see Appendix A below.

NOTE 2 for WC 7132: cert_P35_WC7132-STD_EXEC.zip and cert_P35_WC7132-PS_EXEC.zip are self-extracting executables. Each executable utilizes the Firmware Update Tool as described in Appendix B below. Installing from CentreWare Web is not supported for this product. If CentreWare Web is being used, do not use the .EXE. Instead, use the cert_P35_WC7132-STD_BIN.zip or cert_P35_WC7132-PS_BIN.zip file.

For WC 7228/7235/7245 use WC7228_7235_7245_EXEC.zip or cert_P35_WC7228_7235_7245_BIN.zip (See Note 1 for WC 7228/7235/7245 below)

	If Your Software Version Is Controller ROM	Ready for Patch?	Next step:	Then:	Controller ROM Will Now Show:
1	1.220.0 to below 1.221.9	Yes	Load patch (See Note 1 for WC 7228/7235/ 7245 below)	-	1.221.9

NOTE 1 for WC 7228/7235/7245: cert_P35_WC7228_7235_7245_EXEC.zip is a self-extracting executable that utilizes the Firmware Update Tool as described in Appendix B below. If CentreWare Web is being used, do not use the .EXE. Instead, use the cert_P35_WC7228_7235_7245_BIN.zip file.

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) should be installed by the customer. There are a variety of methods available for this.

- Use the self-extracting executable file which will utilize the Firmware Update Tool. See Appendix B.
- Use XDM/Centreware Web to send Upgrade / Patch files to several devices. For additional information on this method refer to Customer Tip "How to Upgrade, Patch or Clone Xerox Multifunction Devices" (http://www.office.xerox.com/support/dctips/dc06cc0410.pdf)

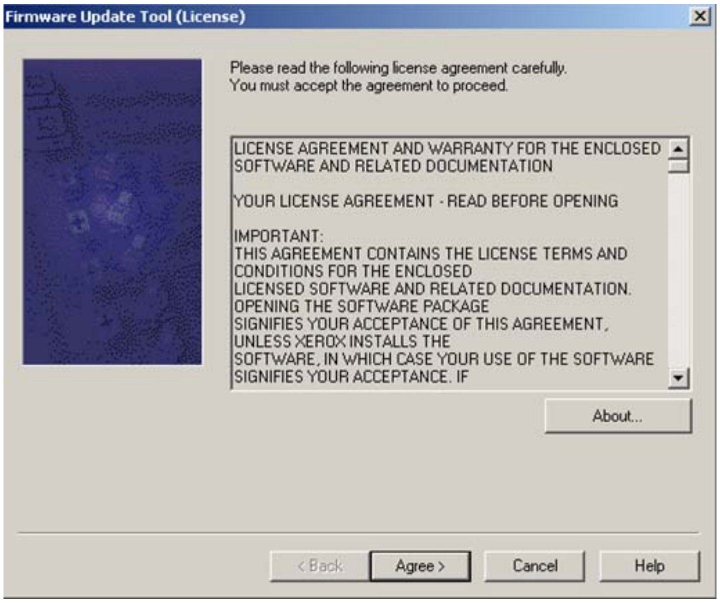
Appendix A – How to determine if the WC 7132 device is configured as PS or STD:

It is important to obtain the correct upgrade file for your machine. Determine the software version you are currently running, as follows:

1. Open your web browser and enter http:// and the TCP/IP address of the machine in the Address or Location field, then press [Enter].
2. Click the [Properties] tab.
3. Click [Configuration].
4. Scroll down to the Software section to see your Controller version. Note whether the Controller ROM is listed as Controller ROM or Controller+PS ROM. This will determine which file to download from Xerox.com. Controller ROM requires the STD file to be loaded. Controller+PS ROM requires the PS file to be loaded.

Appendix B – Using the Firmware Update Tool (self-extracting .EXE):

1. The Firmware Update Tool is supported for only the Windows operating systems. If you do not have a Windows operating system, call Xerox Service for a technician to load the patch.
2. The Firmware Update Tool uses Port 9100. Therefore, make sure Port 9100 is enabled on the device. To do this:
    a. Open your web browser and enter http:// and the TCP/IP address of the machine in the Address or Location field of your browser. Press [Enter].
    b. Click the [Properties] tab.
    c. Click [Port Status].
    d. Make sure the checkbox for "Port 9100" is checked (enabled). If not, check the box and then press [Apply] at the bottom of the web page.
3. Before proceeding with the upgrade, make sure the device is not in use. This includes any jobs in progress and anyone programming a job at the Local User Interface.
4. Double-click on the .EXE filename. You will see the figure below. After reading the License Agreement, press [Agree] to proceed with installation. If upgrading a WC 7132, please make sure the correct file is chosen (PS or STD) by following the instructions in Appendix A above.



Firmware Update Tool (License)

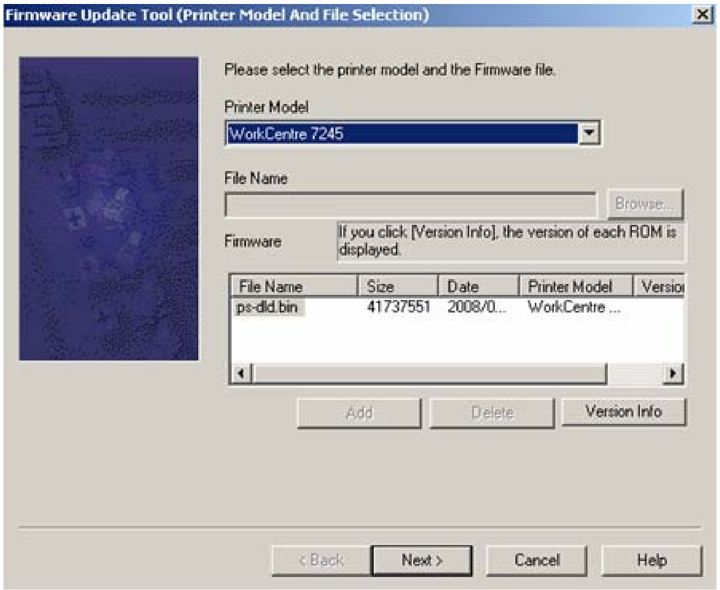
Please read the following license agreement carefully.
You must accept the agreement to proceed.

LICENSE AGREEMENT AND WARRANTY FOR THE ENCLOSED SOFTWARE AND RELATED DOCUMENTATION

YOUR LICENSE AGREEMENT - READ BEFORE OPENING

IMPORTANT:
THIS AGREEMENT CONTAINS THE LICENSE TERMS AND CONDITIONS FOR THE ENCLOSED LICENSED SOFTWARE AND RELATED DOCUMENTATION. OPENING THE SOFTWARE PACKAGE SIGNIFIES YOUR ACCEPTANCE OF THIS AGREEMENT, UNLESS XEROX INSTALLS THE SOFTWARE, IN WHICH CASE YOUR USE OF THE SOFTWARE SIGNIFIES YOUR ACCEPTANCE. IF

5. On the next screen, select the proper Printer Model from the drop-down list. WC 7228/7235/7245 will have the following selections: WorkCentre 7228, WorkCentre 7235, WorkCentre 7245. Make sure the correct model is selected for your device. WC 7132 will have the following selection: WorkCentre 7132.



Firmware Update Tool (Printer Model And File Selection)

Please select the printer model and the Firmware file.

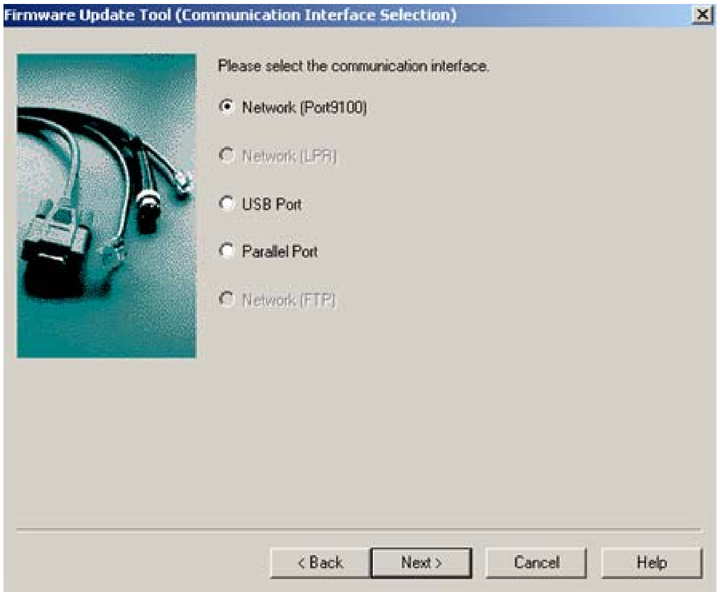
Printer Model: WorkCentre 7245

File Name:

Firmware: If you click [Version Info], the version of each ROM is displayed.

File Name	Size	Date	Printer Model	Versio
ps-dld.bin	41737551	2008/0...	WorkCentre ...	

6. Make sure “Network (Port9100) is selected and press [Next].



Firmware Update Tool (Communication Interface Selection)

Please select the communication interface.

● Network (Port9100)

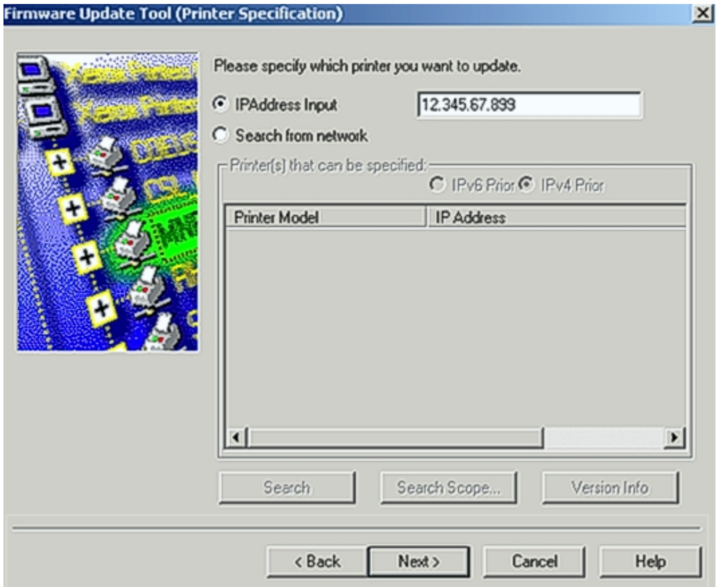
○ Network (LPR)

○ USB Port

○ Parallel Port

○ Network (FTP)

7. Select "IPAddress Input" and type in the TCP/IP Address for the device. Press [Next]. If you chose the incorrect printer model in Step 5 above, you will not be allowed to proceed after pressing {Next}.



Firmware Update Tool (Printer Specification)

Please specify which printer you want to update.

● IPAddress Input 12.345.67.899

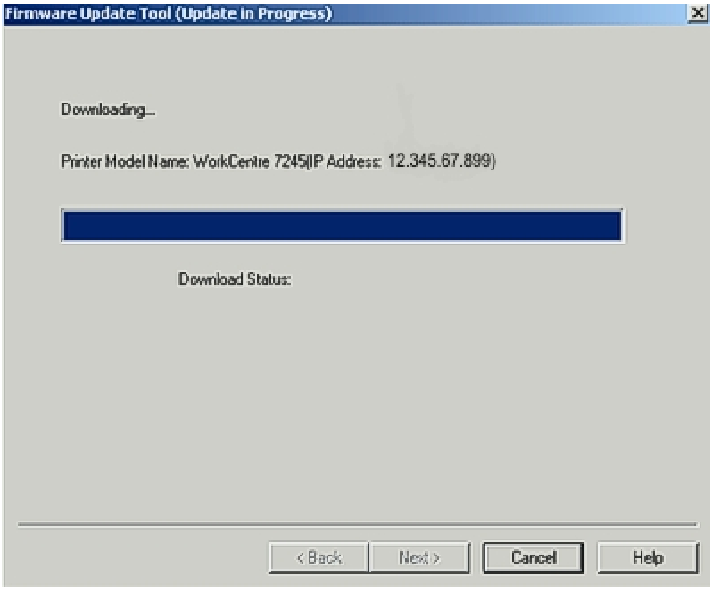
○ Search from network

Printer(s) that can be specified:

○ IPv6 Prior ● IPv4 Prior

Printer Model	IP Address

8. The patch will proceed to be loaded on the device. This will take about 10-15 minutes to complete.



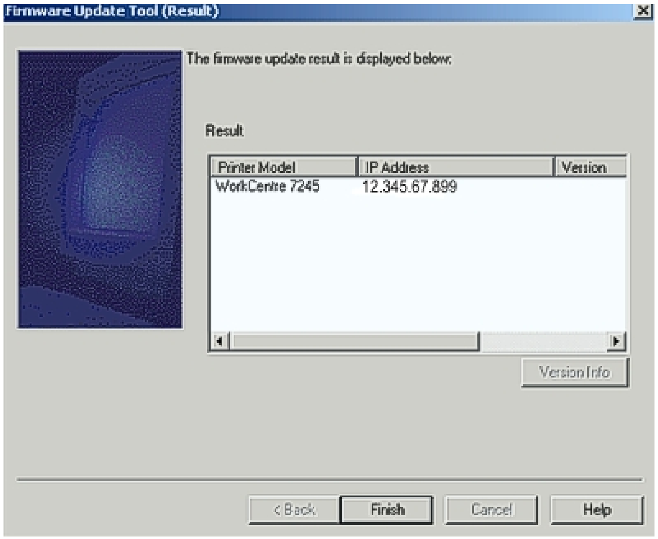
Firmware Update Tool (Update In Progress)

Downloading...

Printer Model Name: WorkCentre 7245(IP Address: 12.345.67.899)

Download Status:

9. Do not press any buttons on the Firmware Update Tool until the “Firmware Update Result is Displayed Below” screen appears. Check the status of the upgrade by scrolling to the right to make sure the device is updated successfully. If successful, press [Finish] to exit the tool. If unsuccessful, make sure the correct file was chosen, the device was not in use at the time of the upgrade, and that the network is functioning properly. If after checking these and upgrade problems still result, contact your local Customer Service Center.

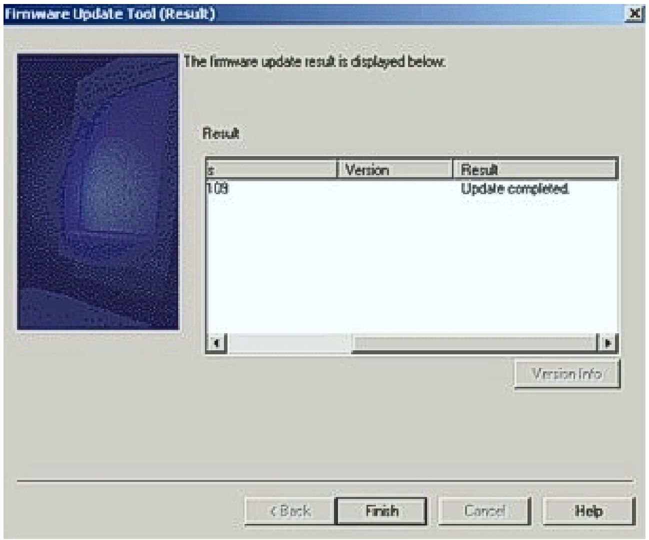


Firmware Update Tool (Result)

The firmware update result is displayed below.

Result

Printer Model	IP Address	Version
WorkCentre 7245	12.345.67.899	



Firmware Update Tool (Result)

The firmware update result is displayed below.

Result

s	Version	Result
109		Update completed.

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 no allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.