Xerox Security Bulletin XRX08-005

Software update to address cross-site scripting vulnerability

v1.0
06/12/08

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.

Louhi Networks of Finland reported this vulnerability to us privately. 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] files containing the 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 languages[2], and can be accessed via the links below or via the links following this bulletin on http://www.xerox.com/security:

- Group 1 Languages Standard -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC123_128_133-STD-G1_EXEC.zip
- Group 1 Languages with Postscript-- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC123_128_133-PS-G1_EXEC.zip
- Group 2 Languages Standard -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC123_128_133-STD-G2_EXEC.zip
- Group 2 Languages with Postscript -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC123_128_133-PS-G2_EXEC.zip
- Group 3 Languages Standard -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC123_128_133-STD-G3_EXEC.zip
- Group 3 Languages with Postscript -- http://www.xerox.com/downloads/usa/en/c/cert_P35_WC123_128_133-PS-G3_EXEC.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[3] of the following products:

WorkCentre®	WorkCentre® Pro
M123	123
M128	128
133	133

[1] Firmware Update Tool for Windows – a firmware upgrade utility bundled with the software release that enables customer installation of the software release
[2] See the Installation Instructions in Appendix B for the list of languages included in Groups 1, 2 and 3
[3] If the product is not connected to the network, it is not vulnerable and therefore no action is required.

Solution

Patch Install Process
Edited: 05/27/08

The P35 patch software only needs to be applied to the MFD if the System Software version of your MFD falls within the range listed.

You must download the patches. The patches are packaged in a ZIP format. Download the zip file from the URL provided and extract all contents to your hard drive. DO NOT TRY TO OPEN THE FILE WITH THE .EXE EXTENSION. The Patch files must not be modified from their original state.

For more detailed instructions on patching WorkCentre devices, please see the Customer Tip: "How to Upgrade, patch or Clone Xerox Multifunction Devices" at: http://www.office.xerox.com/support/dctips/dc06cc0410.pdf.

Install Instructions

Patch filenames for WC M123/M128, WCP 123/128, WC 133, and WCP 133:

- **cert_P35_WC123_128_133-STD-G1_EXEC.zip**
- **cert_P35_WC123_128_133-PS-G1_EXEC.zip**
- **cert_P35_WC123_128_133-STD-G2_EXEC.zip**
- **cert_P35_WC123_128_133-PS-G2_EXEC.zip**
- **cert_P35_WC123_128_133-STD-G3_EXEC.zip**
- **cert_P35_WC123_128_133-PS-G3_EXEC.zip**

	Supported Language	If Your Software Version Is Controller ROM	Ready for Patch?	Next step:	Then:	Controller ROM Will Now Show:
1	G1 (See Note 2 below)	1.202.0 to below 1.206.2	Yes	Load patch (See Notes 1, 2 and 3 below)	-	1.206.2
2	G2 (See Note 2 below)	1.236.0 to below 1.236.2	Yes	Load patch (See Notes 1, 2 and 3 below)	-	1.236.2
3	G3 (See Note 2 below)	1.214.11 to below 1.214.12	Yes	Load patch (See Notes 1, 2 and 3 below)	-	1.214.12

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

NOTE 2: Secondly, it must be determined which software for the desired supported language to load on the device. Supported languages are referred to as G1, G2, and G3. The patch includes G1, G2, or G3 as part of the filename. See Appendix B for the supported languages.

NOTE 3: The patch is a self-extracting executable. Each executable utilizes the Firmware Update Tool as described in Appendix C below. Installing from CentreWare Web is not supported for this product.

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.

Patch Installation Methods

The customer should install this patch and upgrade. To install the patch, use the self-extracting executable file, which will utilize the Firmware Update Tool. See Appendix C.

Appendix A – How to determine if the WC M123/M128, WCP 123/128, WC 133, WCP 133 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.

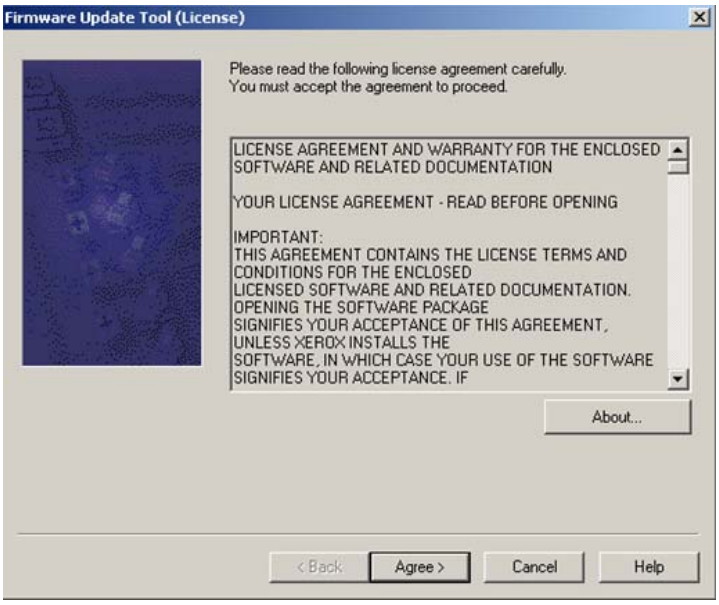
Appendix B – How to determine the desired supported language:

The filename includes an indicator for the supported language. G1, G2, or G3 will be part of the filename. Determine which file from the table below that you will need.

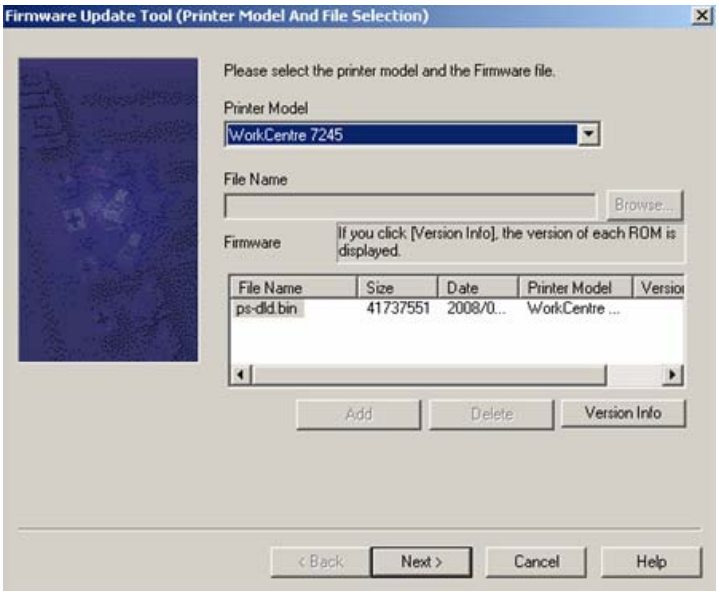
G1 Support Languages	G2 Support Languages	G3 Supported Languages
International English	International English	International English
International French	International French	Hebrew
German	Russian	
Italian	Turkish	
International Spanish	Greek	
Br Portuguese	Czech	
Dutch	Polish	
Danish	Hungarian	
Norwegian	Romanian	
Swedish		
Finnish		

Appendix C – 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. Please make sure the correct file is chosen (PS or STD and correct language (G1, G2, or G3) by following the instructions in Appendix A and Appendix B above.

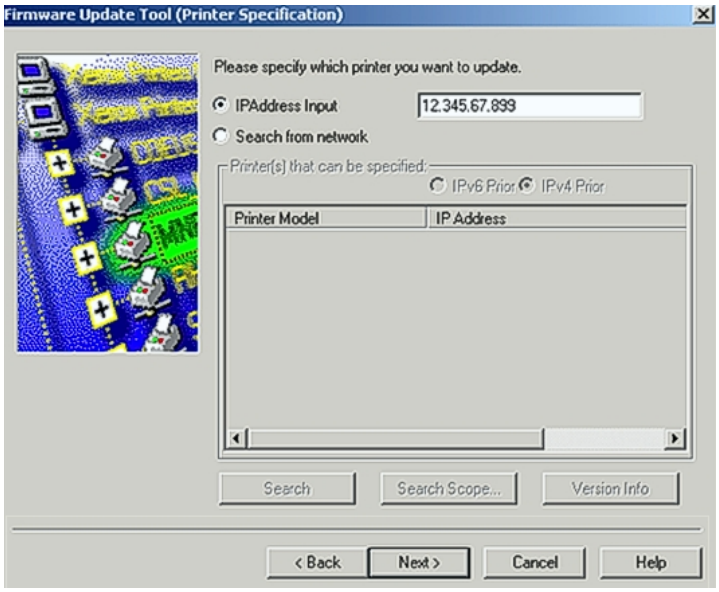


5. On the next screen, select the proper Printer Model from the drop-down list. The following selections will be listed:
    a. CopyCentre/WorkCentre M123
    b. CopyCentre/WorkCentre M128
    c. WorkCentre Pro 123
    d. WorkCentre Pro 128
    e. CopyCentre/WorkCentre 133
    f. WorkCentre Pro 133

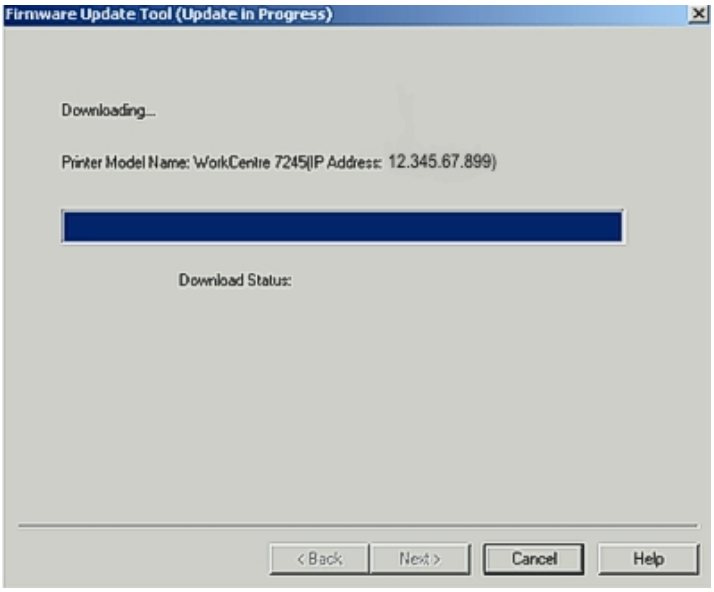


6. Make sure “Network (Port9100) is selected and press [Next].

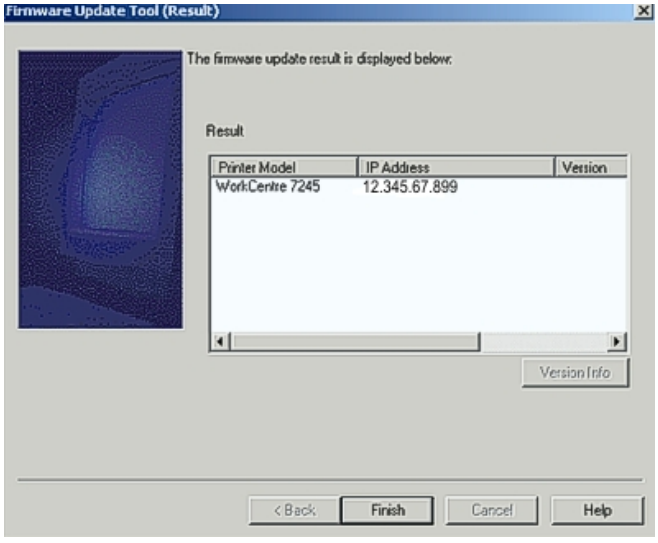
7. Select “IPAddress Input” and type in the TCP/IP Address for the device. Press [Next]. If you chose the incorrect printer model in Step 5 above, you will not be allowed to proceed after pressing {Next}.

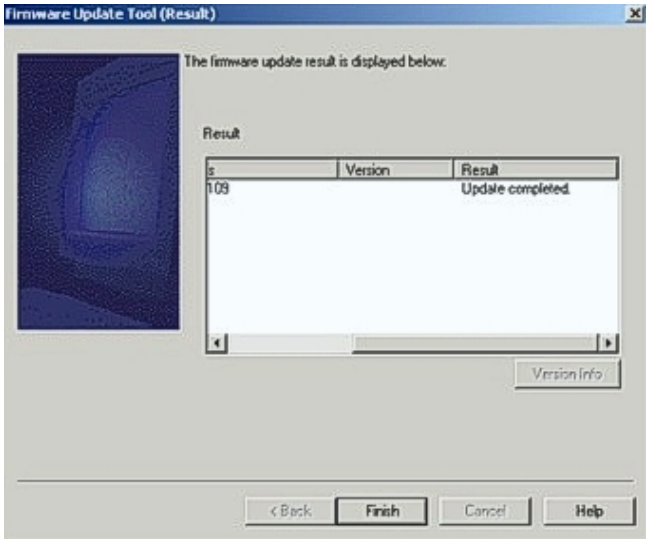


8. The patch will proceed to be loaded on the device. This will take about 10-15 minutes to complete.



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.





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.