Xerox Security Bulletin XRX09-001

Software update to address Command Injection Vulnerability

v1.0
01/30/09

Background

A command injection vulnerability exists in the Web Server of the products listed below. If exploited, the vulnerability could allow remote attackers to execute arbitrary code via carefully crafted inputs on the affected web page. Customer and user passwords are not exposed.

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 0.2 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/downloads/usa/en/c/cert_P37v1_WCP275_WC5687_Patch.zip

This solution is classified as an **Important** patch.

Products affected by this vulnerability are:

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

Install Instructions
Edited: 01/02/09

Install Instructions

Patch file name: **WCP275_WC5687_P37v1.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		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
	System SW or	ESS Controller				
1	*.60.22.006 and earlier	040.022.#1100 and below	N/A – these versions do not have a problem	-	-	-
2	*.60.22.008 to *.60.22.040	040.022.#1120 to 040.022.#1200	Yes	Load P37 patch	-	040.022.#1120.BIOSxx.xx.P37v1 to 040.022.#1200.BIOSxx.xx.P37v1
3	Above *.60.22.040	Above 040.022.#1200	N/A – fix is already in the software	-	-	-

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

	If Your Software Version Is		**Ready for Patch?**	**Next step:**	**Then:**	**Network Controller/ESS Will Now Show:**
	System SW or	**Net Controller**				
1	21.113.02.004 and earlier	050.060.50861 and below	N/A – these versions do not have a problem	-	-	-
2	21.113.02.005 to 21.113.02.04x	050.060.50871 to 050.060.5095x	Yes	Load P37 patch	-	050.060.50871.BIOSxx.xx.P37v1 to 050.060.5095x.BIOSxx.xx.P37v1
3	21.113.02.050 and above	050.060.50960	N/A – fix is already in the software	-	-	-

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_WC5687_P37v1.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 **.P37v1** is appended to the Network Controller (ESS) version number.

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