XEROX SECURITY BULLETIN XRX06-007 (This bulletin is rescinded)

NOTE: Because of intermittent post-installation issues at some customer sites with the P29 security patch (such as the IP configuration of the device becoming disabled or the restrictiveness of the character set used to implement the P29 patch causing problems) it was decided that the P29 patch would be rescinded and no longer made unavailable. Customers experiencing any post-installation issues with the P29 patch or concerned about the vulnerability listed below should contact the Xerox Customer Support Center.

A command injection vulnerability exists in the ESS/ Network Controller and MicroServer Web Server. If exploited this vulnerability could allow remote execution of arbitrary software.

The following software solution (patch P29) and self-service instructions are provided for the listed products. This bulletin covers the same vulnerability as documented in Security Bulletin XRX06-005 but applies to the products listed below. This patch is designed to be installed by the customer. Please follow the procedures below to install the patch to protect your confidential data from possible attack through the network.

The software solution is compressed into a 1 MB zip file and can be accessed in the link following this bulletin on Xerox.com / Security.
Note: The software solution download link for the P29 patch has been made permanently unavailable.

Background
As part of Xerox's on-going efforts to protect customers the following vulnerability was discovered:
* TCP/IP hostname on the Web User Interface vulnerable to command injection

This vulnerability in the ESS/ Network Controller and web server code could allow an attacker to bypass authentication and remotely execute arbitrary software. If successful, an attacker could make unauthorized changes to the system configuration. Customer and user passwords are not exposed.

Acknowledgments:
Xerox wishes to thank:
* Brendan O'Connor for initially notifying us of related vulnerabilities.

This Patch Applies To network-connected versions of the following products:

Document Centre®	WorkCentre®	WorkCentre Pro®
220	M35	35
230	M45	45
240	M55	55
255	M165	65
265	M175	75
332		90
340		165
420		175
425		C32
426		C40
430		C2128
432		C2636
440		C3545
460		
470		
480		
490		
535		
545		
555		

Solution

701P46312

WebUI Patch Install Process
Edited: 17-November-2006

The P29 patch software only needs to be applied to the MFD if the System Software version of your MFD falls within the range listed. There are 3 separate patches, each one corresponding to a specific group of MFD's

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 .TGZ EXTENSION. The Patch files must not be modified from their original state.

For more detailed instructions on patching Document Centre / WorkCentre Pro 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 .

Instructions for the WorkCentre M35/M45/M55 – M165/M175 & WorkCentre Pro 35/45/55 - 165/175 - 65/75/90 & WCP C32/C40 , WCP C2128/C2636/C3545 – Patch P29

Patch File Name: **P29-WC_WCPModelsV2.tgz**
Required for **WCP** System Software Versions:

	System Software	**Net Controller/ESS**
WC M35/M45/M55	2.28.11.000 through 2.97.20.076	1.02.129.1 through 1.08.129.1
WCP 35/45/55	3.28.11.000 through 3.97.20.076	1.02.329.1 through 1.08.329.1
WC M35/M45/M55 with PS option	4.28.11.000 through 4.97.20.076	1.02.229.1 through 1.02.229.1
WCP 65/75/90	1.001.00.060 through 1.001.02.722	1.00.60.3 through 1.08.022.01
WC M165/M175	6.47.39.000 through 6.57.33.017	1.03.464.2 through 1.03.482.1
WCP 165/175	7.47.39.000 through 7.57.33.017	1.03.664.2 through 1.03.682.1
WC M165/M175 with PS option	8.47.30.000 through 8.57.33.017	1.03.564.2 through 1.03.582.1
WCP C32/C40	1.001.00.060 through 1.001.02.723	1.00.60.3 through 1.08.023.01
WCP C2128/C2636/C3545	1.001.04.044 through 0.001.4.519	3.04.044.01 through 3.04.519.02

NOTE: If your WC/WCP device has a higher System Software or Net Controller/ESS version, then you do not need to install the patch.

Confirm your System Software Version

To determine your System Software version, you can either print a Configuration Report or view the version on the Web client interface.
To print a Configuration Report from the local User Interface at the machine:
1) Press the Machine Status button
2) Select Print Configuration Report
3) Look for the System Software Version number.

To view the version from the web client interface:
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.
4) Select "Configuration".
5) Scroll to "Printer Setup" location that displays the System Software Version.

Install the Patch

DO NOT TRY TO OPEN THE PATCH AS IT MAY DAMAGE THE FILE.
This patch can be submitted one of three ways for this model.

1) LPR Method all WCP's
2) Machine Software (Upgrade) Method all WCP's.
3) CentreWare Web. See the Customer Tip referenced above for details.

LPR Method from a Windows NT, 2000, or XP

This method requires that LPR Protocol be enabled on the device. Check the configuration report to see if the protocol is enabled. This protocol can be enabled via the Local User Interface or via the Web Interface. See Appendix A for instructions.

1) Open a "DOS Command Prompt". You can do this by selecting the Windows "Start" icon, and selecting "Run".
2) Type "cmd" and hit <Enter>.
3) Submit the patch file via the command line: **lpr –S <printer_ip> –Plp P29-WC_WCPModelsV2.tgz**

All WCP's will print a patch install sheet and automatically reboot in order to install the patch. The patch is installed when **.P29** is appended to the Network Controller version number. The WC M series (M35,M45,M55,M165,M175) will NOT append .P29, but the patch is installed. This can also be validated using the System Software or Network Controller/ESS version.

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, **P29-WC_WCPModelsV2.tgz**.
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 **.P29** is appended to the Network Controller version number. The WC M series (M35,M45,M55,M165,M175) will NOT append .P29, but the patch is installed.

Instructions for the Document Centre 535/545/555 Patch P29
Instructions for the Document Centre 240/255/265/460/470/480/490 Patch P29
Instructions for the Document Centre 420/425/426/430/432/440 Patch P29

Patch File Name: **P29-DC555f-440F-490f-265f.tgz**
Required for **Document Center** System Software Versions:

	System Software	Net Controller/ESS
DC 535/545/555	14.52.000 through 27.18.036	0.19.10.047.1 - **19.12.029.1**
DC 460/470/480/490	19.5.026 through 19.5.535	07.19.05.026 through 07.19.05.535
DC 420/426/432/440*	Not Applicable	2.3.0.2 through 2.3.26
DC 425/432/440	Not Applicable	3.0.5.4 through 3.2.47
DC 430	Not Applicable	3.3.24 through 3.3.47
DC 240/255/265	6.03 through 6.32	0.18.1.24 through 0.18.6.82

*see next section for versions lower than 2.2.18
NOTE: If your device has a higher System Software or Net Controller/ESS version, then you do not need to install the patch.

Confirm your System Software Version

To determine your System Software version, you can either print a Configuration Report or view the version on the Web client interface.
To print a configuration report from the local User Interface at the machine:
1) Press the Machine Status button
2) Select Print Configuration Report
3) Look for the System Software Version number.

To view the version from the web client interface:
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 "Configuration".
4) Scroll to "Printer Setup" location that displays the System Software Version.

Install the Patch

DO NOT TRY TO OPEN THE PATCH AS IT MAY DAMAGE THE FILE.
This patch can be submitted one of two ways for this model.
1) LPR Method all DC's
2) Machine Software (Upgrade) Method for DC 460/470/480/490 535/545/555 and the DC 240/255/265 only.

LPR Method from a Windows NT, 2000, or XP

This method requires that LPR Protocol be enabled on the device. Check the configuration report to see if the protocol is enabled. This protocol can be enabled via the Local User Interface or via the Web Interface. See Appendix A for instructions.

1) Open a "DOS Command Prompt". You can do this by selecting the Windows "Start" icon, and selecting "Run". Type "cmd" and hit <Enter>.

2) Submit the patch file via the command line: **lpr –S <printer_ip> –Plp P29-DC555f-440F-490f-265f.tgz**

3) The Document Centres 535/545/555 & Document Centre 240/255/265/460/470/480/490 will automatically reboot in order to install the patch. The patch is installed when **.P29** is appended to the Network Controller version number.

4) For the Document Centre 420/426/430/432/440 models either perform a remote reset or power the device off then on for the patch to install.

NOTE: After automatic reboot, you will need to print a second config page on the Document Centre 240/255/265/460/470/480/490 to post the **.P29** to the Network Controller version.

Machine Software (Upgrade) Method

This method is only applicable to the DC535/545/555, DC490/480/470/460 and DC240/255/265 products.

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, **P29-DC555f-440F-490f-265f.tgz**
6) Select the "Install Software" button.

The Document Centres 535/545/555 & Document Centre 240/255/265/460/470/480/490 will automatically reboot in order to install the patch. The patch is installed when **.P29** is appended to the Network Controller version number.

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that .**P29** is appended to the Net Controller version.

Instructions for the Document Centre 220/230/332/340 Patch P29

Patch File Name: **P29-DC220f-332f-420launch.dlm**
Required for **DC** System Software Versions:

	System Software	Net Controller/ESS
DC 220/230/332/340		**1.12.35.1 through 1.12.87**
DC 420/432/440*		**2.1.2 through 2.2.18**

*see previous section for versions higher than 2.2.18

	System Software	ESS
DC 220/230/332/340	Not Applicable	**1.12.35.1 through 1.12.87**
DC 420/432/440*	Not Applicable	**2.1.2 through 2.2.18**

NOTE: If your device has a higher ESS version, then you do not need to install the patch.

Confirm your ESS Software Version

To determine your ESS Software version, you can either print a Configuration Report or view the version on the Web client interface.
To print a configuration report from the local User Interface at the machine:
1) Press the Machine Status button
2) Select Print Configuration Report
3) Look for the ESS Software Version number

To view the version from the web client interface:
1) Open a web browser and connect to the multifunction device by entering the IP number of the device
2) Select the "Device Index" icon in the upper middle portion of the screen.
3) Select **"Device Profile"**.
4) Scroll to the location that displays the ESS Software Version.

Install the Patch

DO NOT TRY TO OPEN THE PATCH AS IT MAY DAMAGE THE FILE.

LPR Method from a Windows NT, 2000, or XP

This method requires that LPD Protocol be enabled on the device. Check the configuration report to see if the LPD protocol is enabled. This protocol can be enabled via the Local User Interface or via the Web Interface. See Appendix A for instructions.
1) Open a "DOS Command Prompt". You can do this by selecting the Windows "Start" icon, and selecting "Run". Type "cmd" and hit <Enter>.
2) Submit the patch file via the command line: **lpr –S <printer_ip> –Plp P29-DC220f-332f-420launch.dlm**
3) Power the device Off, then On. Wait for device to boot.
4) **Power the device off then on again**.
5) The patch is installed when **.P29** is appended to the 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.

For the Document Centre 240/255/265/420/425/432/440/460/470/480/490/535/545/555 and the WorkCentre / WorkCentre Pro models, 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.

For the Document Centre 220/230/332/340 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 "Device Index" icon in the upper right corner
3) Select "Protocols", then scroll to LPD and select the LPD link.
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) Power the MFD off then on.

Disclaimer

The information 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.