XEROX SECURITY BULLETIN XRX04-005

Vulnerability in the ESS/ Network Controller could potentially permit unauthorized access.

The following software solution and self-service instructions are provided for the listed products to protect your confidential data from possible attacks through the network.

The software solution is compressed into an 8.7 MB file and can be accessed using the following link:

http://www.xerox.com/downloads/usa/en/c/cert_XRX04A_patch.zip

Background

There is vulnerability in the PostScript file interpreter code that could allow unauthorized access to the Network controller directory structure. The vulnerability can be exploited using a specially constructed PostScript file to navigate through the directory. An attacker could retrieve the encrypted password file for the device, and then use password cracking tools offline to break the passwords. If successful, the attacker would potentially have full access to the device. Customer/user passwords are not exposed. The device configuration encrypted password can also be retrieved if the attacker is physically present at the machine to retrieve the password file.

Products Affected:

Document Centre	Document Centre
220	430
230	432
240	440
255	460
265	470
332	480
340	490
420	535
425	545
426	555

PS Directory Traversal Patch Install Process

Edited: 6-Jun-2005

There is a patch available that fixes a PostScript Directory Traversal issue (Patch P9 & P12) identified on Document Centre Multifunction Devices (MFD). The patch software only needs to be applied to the MFD if the Network Controller software version or ESS Version of your MFD falls within the range listed.

You must download the patch from the link provided in the bulletin. 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 .TGZ or DLM EXTENSION. This is the patch and must be installed on the MFD as is.

Section 1 - Instructions for the Document Centre 535/545/555. P9

Patch File Name: **P9v2_ps_DC.tgz**
Required for System Software Versions:
14.52.000 through 27.18.014
If your device has a higher System Software 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 right corner
3) Select “Configuration”.
4) Scroll to the 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
2) Machine Software (Upgrade) Method

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”. Enter “cmd” and hit <Enter>.
2) Submit the patch file via the command line: lpr –S <printer_ip> –P lp **P9v2_ps_DC.tgz**
3) The Document Centre 535/545/555 will automatically reboot in order to install the patch. The patch is installed when **.P9** is appended to the Network Controller version number.

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P9** is appended to the Net Controller 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, **P9v2_ps_DC.tgz**.
6) Select the “Install Software” button.
7) The Document Centre 535/545/555 will automatically reboot in order to install the patch. The patch is installed when **.P9** is appended to the Network Controller version number.

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P9** is appended to the Net Controller version.

Section 3 - Instructions for the Document Centre 460/470/480/490. P9

Patch File Name: **P9v2_ps_DC.tgz**

This patch is only needed if your Document Centre falls within the following Net Controller versions:
Version 19.01.037 through 19.05.521 or
Version 19.5.902 through 19.5.912.
If your device has a higher System Software 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 Access button
2) Enter the admin password for the machine
3) Select System Settings
4) Select Configuration Report
5) Select Print Configuration Report
6) Select Close
7) Select Exit
8) 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 right corner
3) Select “Configuration”.
4) Scroll to the 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
2) Machine Software (Upgrade) Method

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”. Enter “cmd” and hit <Enter>.
2) Submit the patch file via the command line: **lpr –S <printer_ip> –P lp P9v2_ps_DC.tgz**
3) The Document Centre 460/470/480/490 will automatically reboot in order to install the patch. The patch is installed when **.P9** is appended to the Network Controller version number.

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P9** is appended to the Net Controller version.

Machine Software (Upgrade) Method

1) Open a web browser and connect to the multifunction device by entering the IP number of thedevice.
2) Select the “Index” icon in the upper right corner.
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, **P9v2_ps_DC.tgz**.
6) Select the “Install Software” button.
7) The Document Centre 460/470/480/490 will automatically reboot in order to install the patch. The patch is installed when **.P9** is appended to the Network Controller version number.

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P9** is appended to the Net Controller version.

Section 4 - Instructions for the Document Centre 420/425/426/430/432/440. P9

Patch File Name: **P9v2_ps_DC.tgz**
This patch is only needed if your Document Centre falls within the following ESS Software versions:
For the DC 420/432/440 with ESS 2.1.2 through 2.3.19 or
For the DC 425/432/440 with ESS 3.0.5.4 through 3.2.29 or
For the DC 430 with ESS 3.3.24 through 3.3.29.
If your device has a higher ESS version, then you do not need the patch.

Confirm your ESS Software Version

To determine your Network Controller 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 Report & Counters
3) Select Print Reports
4) Select Printer Configuration and hit the <Start> button
5) 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 “Index” icon in the upper right corner
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". Enter "cmd" and hit <Enter>.
2) Submit the patch file via the command line: **lpr –S <printer_ip> –P lp P9v2_ps_DC.tgz**
3) Power the device Off, then On OR Reboot the device from the Web client interface*. The patch is installed when **.P9** is appended to the Network Controller version number.

*To reboot the device from the web client interface:

1) Open a web browser and connect to the multifunction device by entering the IP number ofthe device
2) Select the "Status" tab
3) Select the Reboot button
4) Enter the admin username and password of the device
5) Confirm the reboot.

Section 5 - Instructions for the Document Centre 240/255/265. P9

Patch File Name: **P9v2_ps_DC.tgz**

This patch is only needed if your Document Centre falls within the following Net Controller versions:

From 18.6.05 through 18.6.96

If your device has a higher System Software version, then you do not need the patch.

Note: There is no patch for versions 17.4.10 through 17.9.34

Confirm your System Software Version

To determine your Network Controller 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 Access button
2) Enter the admin password for the machine
3) Select System Settings
4) Select Configuration Report
5) Select Print Configuration Report
6) Select Close
7) Select Exit
8) 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 right corner
3) Select "Configuration".
4) Scroll to the 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
2) Machine Software (Upgrade) Method

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". Enter "cmd" and hit <Enter>.
2) Submit the patch file via the command line: **lpr –S <printer_ip> –P lp P9v2_ps_DC.tgz**
3) The Document Centre 240/255/265 will automatically reboot in order to install the patch. The patch is installed when **.P9** is appended to the Network Controller version number.

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P9** is appended to the Net Controller version.

Machine Software (Upgrade) Method

1) Open a web browser and connect to the multifunction device by entering the IP number of the device.
1) Select the "Index" icon in the upper right corner.
2) Select "Machine Software (Upgrades)".
3) Enter the User Name and Password of the device.
4) Under "Manual Upgrade" select Browse button to find and select the file, **P9v2_ps_DC.tgz**.
5) Select the "Install Software" button.

The Document Centre 240/255/265 will automatically reboot in order to install the patch. The patch is installed when **.P9** is appended to the Network Controller version number.
NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P9** is appended to the Net Controller version.

Section 6 - Instructions for the Document Centre 220/230/332/340. P12
Patch File Name: **p12v2_PStrav_DC220-230_DC332-340.dlm**
This patch is only needed if your Document Centre falls within the following ESS Software versions:
1.12.08 through 1.12.85
If your device has a higher ESS version, 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 right corner
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> –P lp p12v2_PStrav_DC220-230_DC332-340.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 **.P12** is appended to the ESS version number.

NOTE: If P12 is not appended to the ESS version number, then you must contact the customer support center to have your machine upgraded to ESS 1.12.85 or the latest available release.

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 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” icon in the upper right corner
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.