

XEROX SECURITY BULLETIN XRX05-008

Vulnerabilities in the Xerox MicroServer Web Server 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 a TBD MB zip file and can be accessed in the link following this bulletin on Xerox.com / Security:

http://www.xerox.com/downloads/usa/en/c/cert_P24_MicroServer_Web_Server_Patch.zip

Background

There are multiple vulnerabilities in the web server code that could allow unauthorized access to the web server including:

- Vulnerabilities that could bypass authentication.
- Specially constructed HTTP requests can cause denial of service or allow unauthorized file access on an attacked machine.
- Cross-site scripting allowing contents of web pages to be modified in an unauthorized manner.

If successful, an attacker could make unauthorized changes to the system configuration. Customer and user passwords are not exposed.

This patch is a cumulative patch that incorporates the security patches documented in Security Bulletins XRX04-002 (P4), XRX05-004 (P11) and XRX05-003 (P16) for the products listed below.

Products Affected:

Document Centre®

240
255
265
420
425
426
430
432
440
460
470
480
490
535
545
555

Solution

WebUI Patch Install Process

Edited: 09-Aug-05

There is a patch available that fixes vulnerabilities in the Xerox MicroServer Web Server that has been identified on Document Centre Multifunction Devices (MFD). The patch software only needs to be applied to the MFD if the System Software version of your MFD falls within the range listed. This patch incorporates earlier patches P4, P11 and P16.

The patch is packaged in a ZIP format. Download the ZIP file from the URL provided and extract all contents to your desktop. The patch should be installed on the devices as specified below. The patch should be sent to the devices as is – do not open the files.

Instructions for the Document Centre 535/545/555

Patch File Name: **P24_http_DC.tgz**

Required for System Software Versions:

14.52.000 through 27.18.029

If your device has 28.18.32 or 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 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
- 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". Type "cmd" and press <Enter>
- 2) Submit the patch file via the command line: **lpr -S <printer_ip> -P lp P24_http_DC.tgz**
- 3) The Document Centre 535/545/555 will automatically reboot in order to install the patch. The patch is installed when **.P24** is appended to the Network Controller version number

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P24** 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, **P24_http_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 **.P24** is appended to the Network Controller version number

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P24** is appended to the Net Controller version.

Instructions for the Document Centre 460/470/480/490

Patch File Name: **P24_http_DC.tgz**

Required for System Software Versions:

Version 19.05.026 through 19.05.528 or

One-Off versions 19.5.902 through 19.05.912

If your device has 19.5.529 or 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 "Software Installed" location that displays the Printer 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". Type "cmd" and press <Enter>

- 2) Submit the patch file via the command line: **lpr -S <printer_ip> -P lp P24_http_DC.tgz**
- 3) The Document Centre 460/470/480/490 will automatically reboot in order to install the patch. The patch is installed when **.P24** is appended to the Network Controller version number

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P24** 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 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, **P24_http_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 **.P24** is appended to the Network Controller version number

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P24** is appended to the Net Controller version.

Instructions for the Document Centre 420/425/426/430/432/440

Patch File Name: **P24_http_DC.tgz**

Required for ESS Versions:

DC 420/426/432/440 with ESS 2.1.2 through 2.3.25

If your device has 2.3.26 or higher ESS version, then you do not need to install the patch.

DC 425/432/440 with ESS 3.0.5.4 through 3.2.40

If your device has 3.2.41 or higher ESS version, then you do not need to install the patch.

DC 430 with ESS 3.3.24 through 3.3.38

If your device has 3.3.41 or 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 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 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 press <Enter>
- 2) Submit the patch file via the command line: **lpr -S <printer_ip> -P lp P24_http_DC.tgz**
- 3) Power the device Off, then On OR Reboot the device from the Web client interface*. The patch is installed when **.P24** is appended to the ESS Software 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 of the 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

Instructions for the Document Centre 240/255/265

Patch File Name: **P24_http_DC.tgz**

Required for System Software Versions:

18.6.05 through 18.6.80 or

One –Off versions 18.6.905 through 18.6.96

If your device has 18.6.82 or higher System Software version, then you do not need to install the patch.

Note: There is no patch for versions 17.4.10 through 17.9.34

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 middle portion of the screen
- 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". Type "cmd" and press <Enter>
- 2) Submit the patch file via the command line: **lpr -S <printer_ip> -P lp P24_http_DC.tgz**
- 3) The Document Centre 240/255/265 will automatically reboot in order to install the patch. The patch is installed when **.P24** is appended to the Network Controller version number

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P24** 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, **P24_http_DC.tgz**
- 6) 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 **.P24** is appended to the Network Controller version number

NOTE: After automatic reboot, you may need to manually print a configuration sheet to see that **.P24** is appended to the Net Controller version.

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 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.