XEROX SECURITY BULLETIN XRX05-009

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_P25_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 patch documented in Security Bulletin XRX04-002 (P4) for the products listed below.

Products Affected:

Document Centre®

220
230
332
340

Solution

WebUI Patch Install Process
Edited: 09-Aug-05

There is a patch available that fixes vulnerabilities in the Xerox MicroServer Web Server that have 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 replaces the earlier patch P4.

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 220/230/332/340

Patch File Name: **P25_http_DC220-340.dlm**
Required for ESS Versions:
1.12.08 through 1.12.85
If your device has 1.12.87 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 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 P25_http_DC220-340.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 **.P25** is appended to the ESS version number

NOTE: If P25 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.

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.