Xerox Security Bulletin XRX10-001

Software update to address Unauthorized Directory Structure Access Vulnerability
v1.0
01/22/10

Background

A vulnerability exists in the Network Controller of the product listed below. If exploited the vulnerability could potentially permit unauthorized access to the Network Controller directory structure via a carefully constructed PostScript file.

A software solution (patch P40) is provided for the product 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 5.3 MB zip file and can be accessed via the link below or via the link following this bulletin announcement on www.xerox.com /security.

http://www.xerox.com/downloads/usa/en/c/cert_WC6400_P40v1_Patch.zip

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

Applicability

This patch applies to network-connected versions[1] only of the following products:

> **WorkCentre®**
> 6400

---

[1]If the product is not connected to the network, it is not vulnerable and therefore no action is required.

Install Instructions

Install Instructions

Patch file name: **WC6400_P40v1.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 6400

	If Your Software Version Is		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
	System SW or	Net Controller				
1	060.070.109.11407 to 060.070.109.29510	060.079.11410 to 060.079.29310	Yes	Load P40 patch	-	060.079.11410.P40v1 to 060.079.29310.P40v1
2	Above 060.070.109.29510	Above 060.079.29310	NA – fix is already in the software	Done	-	-

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 CentreWare 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, **WC6400_P40v1.dlm**.
6) Select the "Install Software" button.
7) All WorkCentres will automatically reboot in order to install the patch. The patch is installed when **.P40v1** is appended to the Network Controller (ESS) version number.

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 not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.