# Xerox Security Bulletin XRX08-006
## Software update to address Web Services vulnerability
v1.0
06/12/08

## Background

A vulnerability exists in the Web Services when attempting to access the Extensible Interface Platform feature under certain conditions.  If exploited this vulnerability could allow an attacker unauthorized access to make changes to the system configuration. Customer and user passwords are not exposed. Xerox is not aware of exploit code existing in the wild.

As part of Xerox's on-going efforts to protect customers, a software solution is provided for the products 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 48 MB zip file and can be accessed via the link below or via the link following this bulletin on [www.xerox.com /security](http://www.xerox.com/security).

[http://www.xerox.com/downloads/usa/en/c/cert_P34v1_WC76xx_Patch.zip](http://www.xerox.com/downloads/usa/en/c/cert_P34v1_WC76xx_Patch.zip)

These solutions are classified as a **Critical** patch.

Note: This security patch is designated as patch **P34**. Once this patch is successfully installed, the Network Controller version will display. BIOSxx.xx.P34v1 (Ex. 040.033.50500 BIOSxx.xx.P34v1). (where xx.xx is the BIOS version, which can differ by machine)

**This software solution applies to network-connected versions[1] of the following products:**

> **WorkCentre®**
>> 7655
>> 7665
>> 7675

---

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

**Patch Install Process**
**Edited: 05/15/08**

## Install Instructions
Patch file name: **cert_P34v1_WC76xx_Patch.dlm**

**This patch can be installed to your systems as outlined below.**

**For WorkCentre® 7655/7665/7675**

| | If Your Software Version Is | | Ready for Patch? | Next step: | Then: | Network Controller/ESS Will Now Show: |
|---|---|---|---|---|---|---|
| | System SW or | Net Controller | | | | |
| 1 | 040.032.xxxxx | 040.032.xxxxx | N/A | Done | - | - |
| 2 | 040.033.50500 to 040.033.53002 | 040.033.50500 to 040.033.53002 | Yes | Load P34 patch | - | 040.033.50500.BIOSxx.xx.P34v1 to 040.033.53002.BIOSxx.xx.P34v1 |
| 3 | 040.033.53011 and higher | 040.033.53011 and higher | N/A | 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 CenterWare 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, **cert_P34v1_WC76xx_Patch.dlm**.
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 **.P34v1** is appended to the Network Controller (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.

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) Enter the user name Admin and the admin password, then select OK.
4) Select "LPR/LPD" or "Line Printer Daemon"
5) If the Enabled box is NOT checked, select the box to add a check mark.
6) Select "Apply New Settings"
7) Reboot the MFD either from the Status web page or by pressing the Power Off button at the MFD.

## Disclaimer