Xerox Security Bulletin XRX11-002

Software Update to Address Buffer Overflow

v1.0
03/25/11

Background

A vulnerability documented in CVE-2010-2063 exists that, if exploited, could allow remote attackers to execute arbitrary code via specially crafted fields in a Service Message Block (SMB) packet. This could occur with buffer overflows in the Samba third-party code that handles file and printer sharing services for SMB clients (including Xerox MFD devices). If successful, an attacker could make unauthorized changes to the system configuration; however, customer and user passwords are not exposed. This vulnerability affects only the printer sharing services.

A software solution (patch P47) 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 update to help protect your product from this issue.

The software solution is compressed into a 1.5 MB zip file and can be accessed via the link below or via the link following this bulletin announcement on http://www.xerox.com/security.

http://www.xerox.com/downloads/usa/en/c/cert_WC57xx_P47v1_Patch.zip

This solution is classified as an **Important** patch[1].

Applicability

The system software releases apply to network-connected versions[2] only of the following products:

WorkCentre®
5735
5740
5745
5755
5765
5775
5790

Note

Even when this patch is properly installed, please be aware that the vulnerability documented in CVE-2010-2063 could still be listed when the software with the P47 patch installed is run against current network vulnerability scanners. This is because current network vulnerability scanners can look for the version of Open Source components like Samba implemented in the software to determine potential vulnerabilities, and the P47 patch does not cause the version of Samba to change. However, if the P47 patch is properly installed the software is protected from the vulnerability documented in CVE-2010-2063 in spite of the vulnerability being reported by a network vulnerability scanner.

---

[1] See the **Security Patch Rating White Paper** for a definition of ratings.

[2] 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: **WC57xx_P47v1.dlm**

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

Summary of versions and actions:

- Determine starting System Software version or Network Controller Version.
- Determine if patch is needed.
- Apply the patch if needed.

	If Your Software Version Is: System SW	Net Controller	Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	061.130.000.04205 to 061.131.201.06200	061.130.06150 to 061.131.06220	Yes	Load P47 patch	-	061.130.06150.P47v1 to 061.131.06220.P47v1
2	061.131.201.06600 and above	061.131.06420 and above	N/A – Fix is already in the software	Done	-	061.131.06420 and above

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 Upgrade.”
4) Enter the User Name and Password of the device.
5) Under “Manual Upgrade” select Browse button to find and select the file, **WC57xx_P47v1.dlm**
6) Select the “Install Software” button.
7) All WorkCentres will automatically reboot in order to install the patch. The patch is installed when **.P47v1** 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.