XEROX SECURITY BULLETIN XRX06-005 (This bulletin is superseded by XRX07-002)

NOTE: Because of intermittent post-installation issues at some customer sites with the P29 security patch (such as the IP configuration of the device becoming disabled or the restrictiveness of the character set used to implement the P29 patch causing problems) it was decided that the P29 patch would be rescinded and no longer made unavailable. The P29 patch is being replaced for the affected products listed below by the P31 patch documented in the Security Bulletin XRX07-002.

A command injection vulnerability exists in the ESS/ Network Controller and MicroServer Web Server. If exploited this vulnerability could allow remote execution of arbitrary software.

The following software solution (patch P29) and self-service instructions are provided for the listed products. This patch is designed to be installed by the customer. Please follow the procedures below to install the patch to protect your confidential data from possible attack through the network.

Note: The software solution download link for the P29 patch has been made permanently unavailable.

Customers concerned about this vulnerability in the products listed below, should first use the attached instructions to verify that they have SMP1 (System Software Version 12.50.03.000, 13.50.03.000, or 14.50.03.000, depending on whether the product is a WorkCentre® or WorkCentre® Pro) or higher. If the System Software Version is not *.50.03.000[1] or above, this software can be obtained from the Drivers & Download section of www.xerox.com. See Appendix A of the Patch Install Instructions to obtain the *.50.03.000 System Software.

Note: This security patch is designated as patch **P29**. Once this patch is successfully installed, the Network Controller version will display the BIOS version of the device and **.P29** (Ex. 40.010.#1172.BIOS07.07.P29[2])

Background

As part of Xerox's on-going efforts to protect customers the following vulnerability was discovered:

- WebUI command injection on TCP/IP hostname

This vulnerability in the ESS/ Network Controller and web server code could allow an attacker to bypass authentication and remotely execute arbitrary software.

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

Acknowledgments:

Xerox wishes to thank:

- Steve Puls, Rajat Mandal and Mike Webb who worked on developing and testing this patch.
- Brendan O'Connor for initially notifying us of related vulnerabilities.

Products This Patch Applies To:

WorkCentre®	WorkCentre® Pro
232	232
238	238
245	245
255	255
265	265
275	275

Note: The WorkCentre® 7655 / 7665 products are not affected by this vulnerability.

[1] * will be either a 12, 13, or 14 depending on whether the product is a WorkCentre® or a WorkCentre® Pro
[2] # will be either a 0, 1, or 5 depending on whether the product is a WorkCentre® or a WorkCentre® Pro

SUPERSEDED

Solution

Install Instructions

Patch file name: **P29_WC2xx-Only_HTTP.dlm**

This patch can be easily installed in a few minutes to your systems as outlined below.

Summary of versions and actions:

	If Your Software Version Is System SW	or Net Controller	Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	*.27.24.000 to *.27.24.014	040.010.#0930 to 040.010.#1110	NO	Upgrade to *.50.03.000	Apply P29 patch	Upgrade first, then see Row 3 below
2	*.27.24.016 to *.27.24.020	040.010.#1120 to 040.010.#1160	Yes	Install P29 patch	Done	040.010.#1120.BIOS07.07.P29 to 040.010.#1160.BIOS07.07.P29
3	*.50.03.000 to *.50.03.009	040.010.#1172 to 040.010.#2250	Yes	Install P29 patch	Done	040.010.#1172.BIOS07.07.P29 to 040.010.#2250.BIOS07.07.P29
4	*.50.03.011 or higher	040.010.#2280 or higher	Fix incorp-orated	Done	-	040.010.#2280 or higher
5	*.27.24.015 Common Criteria Certified	040.010.#1121	Yes	See NOTE 1 below	Done	040.010.#1120.BIOS07.07.P29
6	*.39.24.001 Common Criteria Certified	040.010.#1123	Yes	See NOTE 1 below	Done	040.010.#1123.BIOS07.07.P29

NOTE 1: If your device has a System Software version of either *.27.24.015 or *.39.24.001[3], then your device is in a Common Criteria certified configuration. The device is ready to accept the P29 patch. You can load the P29 patch if desired, although the device would then no longer be in a Common Criteria certified configuration.

SUPERSEDED

[3] **Network Controller Version 040.010.*1121 or 040.010.*1123**

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 Reports”.
3) Select “Print System Configuration Report”.
4) 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.

NOTE 2: If your system software is not within the range of the recommended versions, then go to Appendix A and following the instructions for downloading and updating your system software BEFORE installing the patch.

Install the Patch

1) Open a web browser and connect to the multifunction device by entering the IP address of the device.
2) Select the “Index” icon in the upper right portion of the screen.
3) Select “Manual Upgrade”.
4) Select the Browse button to find and select the file, **P29_WC2xx-Only_HTTP.dlm (Ensure the file is not zipped (P29_WC2xx-Only_HTTP.ZIP.)**
5) Select the “Install Software” button.
6) Enter the User name (Admin) and the Admin Password of the device.
7) The WorkCentre will automatically reboot in order to install the patch.
8) The patch is installed when **.BIOSxx.yy.P29 (xx.yy will be the version of BIOS on your device)** is appended to the Network Controller version number.
   The WorkCentre model will only display the version on the configuration web page and if System Software *.50.03.000 or higher is installed.

This machine has been successfully patched.

SUPERSEDED

Appendix A

Obtaining System Software *.50.03.000

To obtain the latest general release:

a) Use a browser to navigate to www.xerox.com.
b) Select the link called “Support & Drivers”.
c) Select “Multifunction”.
d) Select “WorkCentre” or “WorkCentre Pro” depending on your model.
e) Locate the link for your WorkCentre model.
f) Select “Drivers & Downloads”.
g) Select the link for “Firmware & Machine Upgrades”.
h) Select the link for “System software version *.50.03.000 install instructions” and print or save these instructions.
i) Select the link for “System Software Upgrade Version *.50.03.000” and save the file to your computer.
j) Once downloaded, extract the files to your desktop.
k) Review the “System Software Install Instructions” that you saved.
l) Upgrade the device.
m) Return to the “Install the Patch” section.

<End of instructions>

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.

SUPERSEDED