XEROX 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.

This issue was originally resolved with Security Bulletin XRX06-005. The solution from that bulletin resulted in a patch (P29) and device software that resolved the security issue, but was too restrictive in the number of characters that could be used to configure the devices various network settings. This caused problems for some applications or customers that used special characters, such as the underscore, in their network host names.

Your device may already be protected. If your device meets the minimum software requirements or already has the P29 patch from bulletin XRX06-005 installed and your device is operating properly (e.g., you do not use special characters such as the underscore in your network host names), there is no need to install this patch.

The P31 patch is classified as an **Important** patch.

The software solution is compressed into a 1.1 MB zip file and can be accessed via the link below:
http://www.xerox.com/downloads/usa/en/c/cert_P31v14_ESS_Network_Controller_CP_Patch.zip

This patch is designed to be installed by the customer. Please follow the self-service instructions starting on Page 2 to install the patch to protect your confidential data from possible attack through the network.

Background
As part of Xerox's on-going efforts to protect customers the following vulnerability was discovered:
- TCP/IP hostname on the Web User Interface vulnerable to command injection

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.

This Patch Applies To Network-Connected Versions[1] only of the following products:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
7655	
7665	

---

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

Solution

<div align="center">

WebUI Patch Install Process
Edited: 02-October-2007

</div>

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

Instructions for the WorkCentre®/WorkCentre Pro® 232/238/245/255/265/275

Use patch WCP275_WC7665_P31v14.dlm in file cert_P31v14_ESS_Network_Controller_CP_Patch.zip

	If Your Software Version Is		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
	System SW Controller	or ESS				
1	*.27.24.000 to *.27.24.020	040.010.#0930 to 040.010.#1160	No	Upgrade to *.60.22.000 or higher. See Appendix A on how to obtain this version	See NOTE 1 below	If patch isn't applied 040.022.#1031 If patch is applied 040.022.#1031.BIOSxx.xx.P31v14
2	*.50.03.000 to *.50.03.009	040.010.#1172 to 040.010.#2250	No	Upgrade to *.60.22.000 or higher. See Appendix A on how to obtain this version	See NOTE 1 below	If patch isn't applied 040.022.#1031. If patch is applied 040.022.#1031.BIOSxx.xx.P31v14.
3	*.50.03.011	040.010.#2280	No	Call Service to upgrade to *.60.22.000 or higher	See NOTE 1 below	If patch isn't applied 040.022.#1031 If patch is applied 040.022.#1031.BIOSxx.xx.P31v14
4	*.27.24.015 Common Criteria Certified	040.010.#1121	No	Upgrade to *.60.17.000	See NOTES 1 and 2 below	040.022.#0115
5	*.39.24.001 Common Criteria Certified	040.010.#1123	No	Upgrade to *.60.17.000	See NOTES 1 and 2 below	040.022.#0115
6	*.60.15.000	040.022.#0112	No	Upgrade to *.60.22.000 or higher See Appendix A	See NOTE 1 below	If patch isn't applied 040.022.#1031. If patch is applied 040.022.#1031.BIOSxx.xx.P31v14.
7	*.60.17.000 Common Criteria Certified	040.022.#0115	Yes	See NOTES 1 and 2 below	N/A	If patch is applied, 040.022.#0115.P31v14

	If Your Software Version Is		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
	System SW or Controller	ESS				
8	*.60.17.000 to *.60.22.005	040.022.#0115 to 040.022.#1090	Yes	See NOTE 1 below	N/A	If patch isn't applied 040.022.#1031 to 040.022.#1090. If patch is applied 040.022.#1031.BIOSxx.xx.P31v14 to 040.022.#1090.BIOSxx.xx.P31v14.
9	"*.60.22.006 and above	040.022.#1100 or above	N/A	Done	N/A	N/A

Instructions for the WorkCentre® 7655/76655

Use patch WCP275_WC7665_P31v14.dlm in file cert_P31v14_ESS_Network_Controller_CP_Patch.zip

	If Your Software Version Is		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
	System SW or	Net Controller				
1	040.032.50855 to 040.032.51040	040.032.50855 to 040.032.51030	No	Call Service to Upgrade to 040.032.53080	See NOTE 1 below	If the patch is applied, 040.032.53080.BIOSxx.xx.P31v14
2	040.032.53080 Common Criteria Certified	040.032.53080	Yes	See NOTES 1 and 2 below	N/A	If patch is applied, 040.032.53080.BIOSxx.xx.P31v14
3	040.032.55030 to 040.032.55061	040.032.55030 to 040.032.55060	Yes	See NOTE 1 below	N/A	If patch is applied, 040.032.55030.BIOSxx.xx.P31v14 to 040.032.55060.BIOSxx.xx.P31v14
4	040.032.55070 and above	040.032.55070	N/A	Done	N/A	N/A

NOTE 1: Your device is now protected against the security issue noted in this bulletin. However, if you find that the character restrictions contained in the release are too restrictive for your environment and you would like to implement a less restricted character set (while still maintaining protection against this security issue), load the P31 patch **WCP275_WC7665_P31v14.dlm** onto your device.

NOTE 2: Your device is in a Common Criteria certified configuration. If you do load the P31 patch **WCP275_WC7665_P31v14.dlm** onto your device to implement a less restricted character set per Note 1, your device would then no longer be in a Common Criteria Certified configuration.

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.

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 appropriate file **WCP275_WC7665_P31v14.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 **.P31vxx** is appended to the Network Controller (ESS) version number.

Appendix A - Obtaining System Software Version *.60.22.000 or later

To obtain system software versions *.60.22.000 or later:

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 set *.60.22.000 install instructions" and print or save these instructions.

i) Select the link for "System Software set *.60.22.000" 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.

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.