

Xerox Security Bulletin XRX09-002

Software update to address Command Injection Vulnerability

v1.0
05/15/09

Background

A command injection vulnerability exists in the Web Server of the products listed below. If exploited, the vulnerability could allow remote attackers to execute arbitrary code via carefully crafted inputs on the affected web page. Customer and user passwords are not exposed.

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 an 8.1 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/downloads/usa/en/c/cert_P38v1_WCP275_WC7675_WC5687_Patch.zip

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

Products affected by this vulnerability are:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
5632	
5638	
5645	
5655	
5665	
5675	
5687	
7655	
7665	
7675	

Install Instructions

Install Instructions

Patch file name: WCP275_WC7675_WC5687_P38v1.dlm.dlm

This patch can be installed on 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/WCP 232/238/245/255/265/275

	If Your Software Version Is System SW or ESS Controller	Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:	
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	Load P38 patch	040.022.#1031.BIOSxx.xx.P38v1
2	*.39.24.001	040.010.#1123	No	Upgrade to *.60.22.000 or higher. See Appendix A	Load P38 patch	040.022.#1031.BIOSxx.xx.P38v1
3	*.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	Load P38 patch	If patch is applied 040.022.#1031.BIOSxx.xx.P38v1
4	*.50.03.011	040.010.#2280	No	Call Service to upgrade to *.60.22.000 or higher	Load P38 patch	If patch is applied 040.022.#1031.BIOSxx.xx.P38v1
5	*.60.15.000	040.022.#0112	No	Upgrade to *.60.22.000 or higher See Appendix A	Load P38 patch	040.022.#1031.BIOSxx.xx.P38v1
6	*.60.17.000 to *.60.18.000	040.022.#0115 to 040.022.#1031	No	Upgrade to *.60.22.000 or higher See Appendix A	Load P38 patch	040.022.#1031.BIOSxx.xx.P38v1
7	*.60.22.000 to *.60.22.044	040.022.#1031 to 040.022.#1202	Yes	Load P38 patch	-	040.022.#1031.BIOSxx.xx.P38v1 to 040.022.#1202.BIOSxx.xx.P38v1
8	*.60.22.050 and above	040.022.#1210 or above	N/A – fix is already in the software	Done	-	-



For WC 7655/7665/7675

	If Your Software Version Is System SW or Net Controller		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	040.032.xxxxx	040.032.xxxxx	No	Call Service to Upgrade to 040.033.53050	Load P38 patch	040.033.53050.BIOSxx.xx.P38v1
3	040.033.50500 to 040.033.51010	040.033.50500 to 040.033.51010	No	Upgrade to 040.033.53050	Load P38 Patch	040.033.53050.BIOSxx.xx.P38v1
4	040.033.52800 to 040.033.53102	040.033.52800 to 040.033.53102	Yes	Load P38 patch	-	040.033.52800.BIOSxx.xx.P38v1 to 040.033.53102.BIOSxx.xx.P38v1
5	040.033.53110 and above	040.033.53110	N/A – fix is already in the software	Done	-	-

For WC 5632/5635/5645/5655/5665/5675/5687

	If Your Software Version Is System SW or Net Controller		Ready for Patch?	Next step:	Then:	Network Controller/ESS Will Now Show:
1	21.105.01.000	050.060.50730	No	Upgrade to 21.113.02.000	Load P38 patch	050.060.50812.BIOSxx.xx.P38v1
2	21.113.02.000 to 21.113.02.060	050.060.50812 to 050.060.50980	Yes	Load P38 Patch	-	050.060.50812.BIOSxx.xx.P38v1 to 050.060.50980.BIOSxx.xx.P38v1
3	Above 21.113.02.060	Above 050.060.50980	N/A – fix is already in the software	Done	-	-
4	21.120.xx.xxx	060.10x.xxxxx	N/A – fix is already in the software	Done	-	-
5	25.054.xxx.xxx	060.06x.xxxxx	N/A – 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.
- Use 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, **WCP275_WC7675_WC5687_P38v1.dlm**.
- 6) Select the "Install Software" button.
- 7) All WCPs will print a patch install sheet and automatically reboot in order to install the patch. The patch is installed when **.P38v1** 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.