1

Xerox Security Bulletin XRX12-003

Address Postscript and DLM Vulnerabilities

v1.1
03/07/12

Background

Vulnerabilities exist that, if exploited, could allow remote attackers to insert arbitrary code into the device. This could occur with a specifically crafted Postscript or firmware job submitted to the device. If successful, an attacker could make unauthorized changes to the system configuration; however, customer and user passwords are not exposed.

As part of Xerox's on-going efforts to protect customers, the ability to accept these specially crafted jobs can be disabled for the network-connected versions[1] of affected products listed below as follows:

1. Software upgrades can be disabled at the device by an administrator[2]:
    - ColorQube 9201/9202/9203
    - ColorQube 9301/9302/9303
    - Phaser 3635MFP
    - Phaser 4600/4620
    - Phaser 6700
    - Phaser 7800
    - WorkCentre 232/238/245/255/265/275
    - WorkCentre 4150
    - WorkCentre 4250
    - WorkCentre 4260
    - WorkCentre 5030/5050
    - WorkCentre 5135/5150
    - WorkCentre 5222/5225/5230
    - WorkCentre 5325/5330/5335
    - WorkCentre 5632/5638/5645/5655/5665/5675
    - WorkCentre 5735/5740/5745/5755/5765/5775/5790
    - WorkCentre 6400
    - WorkCentre 7120/7125
    - WorkCentre 7132
    - WorkCentre 7228/7235/7245
    - WorkCentre 7232/7242
    - WorkCentre 7328/7335/7345/7346
    - WorkCentre 7425/7428/7435
    - WorkCentre 7525/7530/7535/7545/7556
    - WorkCentre 7655/7665/7675
    - WorkCentre 7755/7765/7775
    - WorkCentre Bookmark 40/55
    - WorkCentre M35/M45/M55
    - WorkCentre M165/M175
    - WorkCentre Pro 32/40 Color
    - WorkCentre Pro 35/45/55
    - WorkCentre Pro 65/75/90

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

[2] Notes:

a. Disabling the software upgrade feature also disables the ability of the device to accept clone files.
b. Many of those products listed above already support the ability to disable the Software Upgrade feature through the device web interface. This can be done without requiring loading of any additional software.

- WorkCentre Pro 165/175
- WorkCentre Pro 232/238/245/255/265/275
- WorkCentre Pro C2128/C2636/C3545
- Xerox Color 550/560

2. The device configuration security settings can be set by an administrator to deny access to configuration changes:
   - ColorQube 8570/8870
   - Phaser 4510
   - Phaser 5550
   - Phaser 6350
   - Phaser 6360
   - Phaser 7400
   - Phaser 7500
   - Phaser 7760
   - Phaser 8550
   - Phaser 8560
   - Phaser 8560MFP
   - Phaser 8860
   - Phaser 8860MFP

3. A software patch will be available to add the ability of an administrator to disable software:
   - Phaser 3160N
   - Phaser 3250
   - Phaser 3300MFP
   - Phaser 3435
   - Phaser 3600
   - WorkCentre 3210/3220
   - WorkCentre 3550
   - WorkCentre 4118
   - WorkCentre M20/M20i

4. No action is needed[3]:
   - Document Centre 430
   - Phaser 6115MFP
   - Phaser 6121MFP
   - WorkCentre M118/M118i

5. The following products are under review:
   - Phaser 6010
   - Phaser 6125
   - Phaser 6128MFP
   - Phaser 6130
   - Phaser 6140
   - Phaser 6180
   - Phaser 6180MFP
   - Phaser 6280
   - Phaser 6500
   - WorkCentre 3045N/I
   - WorkCentre 5020
   - WorkCentre 6015N/I
   - WorkCentre 6505
   - WorkCentre Pro 123/128/133

[3] To protect the listed products from the vulnerabilities addressed in this bulletin.

- Xerox 4127/4112
- Xerox 4590/4595

Please follow the applicable procedures below to protect your product from this possible attack through the network.

The solution for this vulnerability is classified as **Critical**.

Acknowledgment

Xerox wishes to thank both Deral Heiland (www.foofus.net) and Andrei Costin (www.andreicostin.com) for initially notifying us of these vulnerabilities.

Process to Disable Software Upgrades

Use the steps listed below for the indicated products to disable software upgrades on the device. Note that in each case only the System Administrator can perform these steps.

For Phaser 3635MFP, WorkCentre 4150 and WorkCentre 4250/4260

To disable software upgrades, perform the following:

1. At your Workstation, open a web browser and enter the IP Address of your machine in the Address Bar.
2. Press **Enter**.
3. Log into the web interface into the 'admin' account with the current System Administrator password.
4. Click on the **Properties** tab.
5. Click on the **Maintenance** link.
6. Click on the **Upgrade Management** link.
7. Make sure the **Enabled** checkbox is not selected; if it is selected click on the checkbox to deselect it.
8. Do not fill in any of the other fields on this web page and do not select the **Install Software** button.
9. Proceed to any other web page.

Software upgrades will now be disabled.

For Phaser 4600/4620

To disable software upgrades, perform the following:

1. At your Workstation, open a web browser and enter the IP Address of your machine in the Address Bar.
2. Press **Enter**.
3. Log in as the 'admin' user and enter the current System Administrator password.
4. Click on the **Properties** tab.
5. Click on the **Maintenance** link.
6. Click on the **Firmware Upgrade** link.
7. Make sure the **Enabled** checkbox is not selected; if it is selected click on the checkbox to deselect it.
8. Do not fill in any of the other fields on this web page and do not select the **Install Software** button.
9. Proceed to any other web page.

Software upgrades will now be disabled.

For ColorQube 9201/9202/9203, ColorQube 9301/9302/9303, Phaser 6700, Phaser 7800, WorkCentre 5135/5150, WorkCentre 5632/5638/5645/5655/5665/5675, WorkCentre 5735/5740/5745/5755/5765/5775/5790, WorkCentre 6400, WorkCentre 7525/7530/7535/7545/7556, WorkCentre 7755/7765/7775 and WorkCentre Bookmark 40/55

To disable software upgrades, perform the following:

1. At your Workstation, open a web browser and enter the IP Address of your machine in the Address Bar.
2. Press **Enter**.
3. Log in as the 'admin' user and enter the current System Administrator password.
4. Click on the **Properties** tab.
5. Click on the **General Setup** link.
6. Click on the **Machine Software** link.
7. Click on the **Upgrades** button.
8. Make sure the **Enabled** checkbox is not selected; if it is selected click on the checkbox to deselect it.
9. Click **Apply**.

Software upgrades will now be disabled.

For WorkCentre 232/238/245/255/265/275, WorkCentre 5030/5050, WorkCentre M35/M45/M55, WorkCentre M165/M175, WorkCentre Pro 35/45/55, WorkCentre Pro 165/175 and WorkCentre Pro 232/238/245/255/265/275

To disable software upgrades, perform the following:

1. At your Local User Interface on the device, press the [**Access**] button to enter the Tools Pathway.
2. Log in as the 'admin' user and enter the current System Administrator password.
3. Touch the [**Go to Tools**] button.
4. Wait for the screen to refresh and touch the [**More**] button.
5. Touch the [**More**] button again.
6. Touch the [**Customer Software Upgrade**] button.
7. Touch the [**Off**] button.
8. Touch the [**Save**] button.
9. Touch the [**Exit Tools**] button to exit the Tools Pathway.

Software upgrades will now be disabled.

For WorkCentre 5222/5225/5230, WorkCentre 5325/5330/5335, WorkCentre 7120/7125, WorkCentre 7132, WorkCentre 7228/7235/7245, WorkCentre 7232/7242, WorkCentre 7328/7335/7345/7346, WorkCentre 7425/7428/7435 and Xerox Color 550/560

To disable software upgrades, perform the following:

1. At the control panel on the device select the **Log In/Out** button.
2. Enter the **System Administrator Login ID** ('admin' username) and System Administrator **Passcode**.
3. Touch **Machine Status** button.
4. Touch the **Tools** tab.
5. Touch the **System Settings**.
6. Touch the **Common Service Settings**.
7. Touch the **Other Settings**.
8. Touch **SW Download**.
9. Select the **Disabled** option.
10. Touch **Save**.

Software upgrades will now be disabled[4]; once upgrades are disabled in this manner no one, even Service, will be able to upgrade the device until upgrades are enabled again.

For WorkCentre 7655/7665/7675

To disable software upgrades, perform the following:

1. At your Local User Interface on the device, press the [**Log In / Out**] button to enter the Tools Pathway.
2. Log in as the 'admin' user and enter the current System Administrator password.
3. Touch the [**Machine Status**] button, then the [**Tools**] tab.
4. Touch the [**Connectivity and Network Setup**] button.
5. Touch the [**General**] button.
6. Touch the [**Remote Software Upgrade**] button.
7. Touch the [**Disable**] button.
8. Touch the [**Save**] button.
9. Touch the [**Log In / Out**] button to exit the Tools Pathway.

Software upgrades will now be disabled.

[4] Disabling Upgrade via CenterWare Internet Services (CWIS) will only disable network upgrades initiated via CWIS; you will still be able to upgrade the machine via USB or LPR.

For WorkCentre Pro 32/40 Color

To disable software upgrades, perform the following:

1. At your Local User Interface on the device, press the [**Access**] button to enter the Tools Pathway.
2. Log in as the 'admin' user and enter the current System Administrator password. Touch the [**Log-In**] button when finished.
3. Wait for the screen to refresh and touch the [**More**] button.
4. Touch the [**More**] button again.
5. Touch the [**Remote Software Upgrade**] button.
6. Touch the [**Off**] button.
7. Touch the [**Save**] button.
8. Touch the [**Exit Tools**] button to exit the Tools Pathway.

Software upgrades will now be disabled.

For WorkCentre Pro 65/75/90

To disable software upgrades, perform the following:

1. At your Local User Interface on the device, press the [**Access**] button to enter the Tools Pathway.
2. Log in as the 'admin' user and enter the current System Administrator password. Touch the [**Enter**] button when finished.
3. Wait for the screen to refresh and touch the [**More**] button.
4. Touch the [**More**] button again.
5. Touch the [**Remote Software Upgrade**] button.
6. Touch the [**Off**] button.
7. Touch the [**Save**] button.
8. Touch the [**Exit Tools**] button to exit the Tools Pathway.

For WorkCentre Pro C2128/C2636/C3545

To disable software upgrades, perform the following:

1. At your Local User Interface on the device, press the [**Access**] button to enter the Tools Pathway.
2. Log in as the 'admin' user and enter the current System Administrator password. Touch the [**Login**] button when finished.
3. Touch the [**Go to Tools**] button, if required.
4. Wait for the screen to refresh and touch the [**More**] button.
5. Touch the [**More**] button again.
6. Touch the [**Customer Software Upgrade**] button.
7. Touch the [**Off**] button.
8. Touch the [**Save**] button.
9. Touch the [**Exit Tools**] button to exit the Tools Pathway.

Software upgrades will now be disabled.

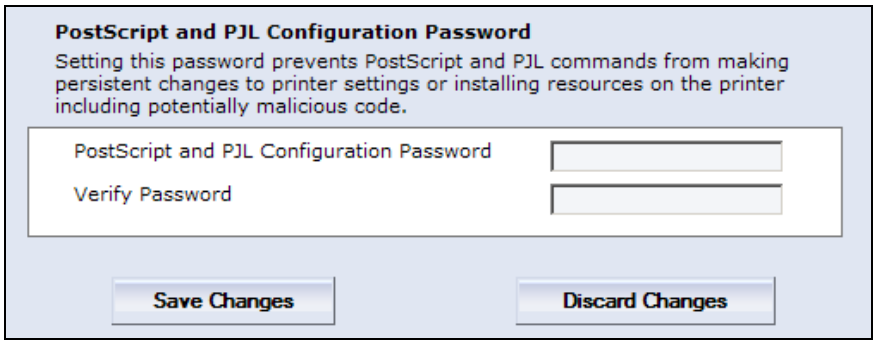
Process to Deny Access to Configuration Changes Made via PostScript and PJL and to Download Firmware

Use the steps listed below for the indicated products to deny access to configuration changes made to the device via PDLs – PostScript and PJL, and as a result deny the ability to download firmware. Note that only the System Administrator can perform these steps.

For ColorQube 8570/8870, Phaser 4510, Phaser 5550, Phaser 6360, Phaser 7500, Phaser 8560 and Phaser 8860

The above listed products support setting of a password that then must be included with the PostScript or PJL job if the job attempts to change printer settings or install or modify resources[5]. This password can be set via CentreWare Internet Services (CWIS) as follows:

1. At your Workstation, open a web browser and enter http://xxx.xxx.xxx.xxx/securitysettings.html, where xxx.xxx.xxx.xxx is the IP Address of the device.
2. Enter the desired password in the PostScript and PJL Configuration Password page shown below:



This will then required this password to be entered to perform the following features:

- Loading of fonts, forms and macros via snippet
- Sys/Start jobs that were performing some function at start time.
- Any postscript or PJL snippet that attempts to change device configuration or modify resources on the device.
- TFTP jobs that use PS configuration files
- Downloading firmware to upgrade the device.

Note that normal print jobs and customer workflows will not be affected.

For Phaser 6350, Phaser 7400, Phaser 7760, Phaser 8550, Phaser 8560MFP and Phaser 8860MFP

The above listed products support a checkbox that allows or denies access to configuration changes made to the device via PDLs – PostScript and PJL, as well as deny downloading firmware. When the box is **unchecked**, no modifying files can be downloaded to the device. This configuration parameter can be set via CentreWare Internet Services (CWIS) as follows:

1. At your Workstation, open a web browser and enter http://xxx.xxx.xxx.xxx/securitysettings.html, where xxx.xxx.xxx.xxx is the IP Address of the device.
2. Uncheck the box in the Language Operator Authorization page shown below:

[5] The Phaser 4510, Phaser 6360, Phaser 8560 and Phaser 8860 require a later firmware release to support the Password password functionality. If you have an older release, the method described for the Phaser 6350 et al below should be used. The PostScript and PJL Configuration functionality was introduced in these products starting with the following versions:

- Phaser 4510: PostScript version 4.11 or later
- Phaser 6360: PostScript version 4.12 or later
- Phaser 8560/Phaser 8860: PostScript version 4.7 or later

This will block the following features:

- Loading of fonts, forms and macros via snippet
- Sys/Start jobs that were performing some function at start time.
- Any postscript or PJL snippet that attempts to change device configuration or modify resources on the device.
- TFTP jobs that use PS configuration files
- Downloading firmware to upgrade the device.

Note that normal print jobs and customer workflows will not be affected.

Process to Disable Ability to Upgrade Internal Software

Use the steps listed below for the indicated products to disable the ability of the device to accept an upgrade of the internal software. Note that only the System Administrator can perform these steps.

For Phaser 3160, Phaser 3250, Phaser 3300MFP, Phaser 3535, Phaser 3600, WorkCentre 3550, WorkCentre 4118 and WorkCentre M20/M20i

1. *Print a configuration page from the printer to verify the printer's current software version. If the software version is the version indicated in the table below, then a new feature is now available to either enable or disable the ability to allow firmware upgrades to the device.* ***NOTE:*** *If the firmware version is lower than the version indicated in the table below, then go to the link indicated in the table to download the current release of software for the applicable device.*

Product	Software Version Containing Ability to Disable Upgrades	Location of Software Releases
Phaser 3160N	To Be Announced	To Be Announced
Phaser 3210/3220	2.50.00.99_R4 or higher[6]	http://www.support.xerox.com/support/workcentre-3210-3220/downloads/enus.html?operatingSystem=win7&fileLanguage=enc
Phaser 3250	1.70.02.41 SMP1-R15 or higher	http://www.support.xerox.com/support/phaser-3250/downloads/enus.html?operatingSystem=win7&fileLanguage=en
Phaser 3300MFP	1.50.00.14_SMP1R16 or higher[4]	http://www.support.xerox.com/support/phaser-3300mfp/downloads/enus.html?operatingSystem=win7
Phaser 3435	To Be Announced	To Be Announced
Phaser 3600	To Be Announced	http://www.support.xerox.com/support/phaser-3600/downloads/enus.html?operatingSystem=win7
WorkCentre 3550	25.002.03.000 or higher[4]	http://www.support.xerox.com/support/workcentre-3550/downloads/enus.html?operatingSystem=win7&fileLanguage=en
WorkCentre 4118	To Be Announced	http://www.support.xerox.com/support/workcentre-4118/downloads/enus.html?operatingSystem=win7&fileLanguage=en
WorkCentre M20/M20i	3.09_R15_1 or higher[4]	http://www.support.xerox.com/support/workcentre-m20-m20i/downloads/enus.html?operatingSystem=win7

2. Open a Web Browser application from a computer that is connected to the same network as the printer. Type in the IP address of the printer in the address bar. Press the **Enter** key to connect to the printer.
3. Click on the **Properties** link.
4. Scroll to the **Security** link on the left-hand side of the page and click on the "+" button to expand the Security options.
5. Click on the **Upgrade Management** link on the left-hand side of the page. If prompted, enter the CWIS user name and password).
6. Make sure the **Enabled** checkbox in the Software Upgrade page is not checked; if it is checked click on the **Enabled** checkbox to deselect it.

[6] English Only

7. Click **Ok** to close the pop-up window.
8. Close your Web Browser.

Software upgrades will now be disabled.

NOTE: If Software Upgrade is disabled then a software upgrade cannot be performed on the printer over any port (FTP, LPR, Port9100, or USB). If your printer is connected via USB to your computer, you will need to connect the printer via Ethernet to re-enable software upgrades if you need to upgrade the printer's software in the future.

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.

©2012 Xerox Corporation. All rights reserved. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation. XEROX®, XEROX and Design®, CentreWare®, Phaser®, ColorQube®, Document Centre®, WorkCentre®, and WorkCentre Pro® are trademarks of Xerox Corporation in the United States and/or other countries. Adobe® and PostScript® are registered trademarks or trademarks of Adobe Systems, Incorporated. All other trademarks are the property of their respective manufacturers.
The information in this bulletin is subject to change without notice.