Xerox Security Bulletin XRX16-007

Card Authentication Error

v1.3
06/15/16

Background

An error in authentication using cards could allow unauthorized access to user print jobs. A solution consisting of software patch 876840v5 is provided that addresses this error for WorkCentre versions 073.xxx.075.34540 and 073.xxx.035.28000 for the affected products.

This software patch is designed to be installed by the customer. The software patch is compressed into a zip file and can be accessed via the link below:

Software Patch: 876840v5.zip -- http://www.support.xerox.com/support/_all-products/file-download/enus.html?contentId=134124

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

Please follow the instructions starting on page 3 for each affected product to install this software patch.

IMPORTANT NOTE: This patch only applies to system software release 073.xxx.035.28000 for the affected products.

Applicability

This patch applies to network-connected versions[1] only of the following products:

WorkCentre®

3655 / 3655i
5845
5855
5865 / 5865i
5875 / 5875i
5890 / 5890i
5945 / 5945i
5955 / 5955i
6655 / 6655i
7220 / 7220i
7225 / 7225i
7830 / 7830i
7835 / 7835i
7845 / 7845i
7855 / 7855i
7970 / 7970i

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

Instructions (What must to be done If I have one of the affected products?)

Determine what actions, if any, need to be performed to prep the device for patch installation and then install the patch:

1. Determine the current System Software version on your device by printing a Configuration Report. To print a Configuration Report follow the instructions for how to print a Configuration Report in the System Administrator Guide for each product in question.
2. Determine if any action needs to be taken based on the System Software version listed on the Configuration Report for each device. This is done by following steps 3 through 6.
3. Determine the appropriate Patch Installation Action Table to follow starting on page 4 by looking for your product number at the top of each chart, and matching it to your specific product.
4. Locate either the System Software version in the chart that matches or falls within the listed Software versions.
5. From the directions in the Patch Installation Action Table for the affected product and System Software version, determine what action(s), if any, have to be taken before the applicable patch can be installed.
6. Perform the indicated action(s) to get your device ready to install the applicable patch.
7. Make sure that Software Upgrade enabled on the device (i.e., turned on) if it is disabled.
8. Once your device is ready to install the applicable patch, follow the instructions below under Install the Patch on page 6 to install the patch on the device.

Patch Installation Action Tables

The following tables indicate what actions, if necessary, are needed before the patch can be installed on an affected device:

For WorkCentre 3655/3655i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.060.035.24100** or less	**073.065.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.065.24100** or less
2	073.060.035.28000	073.065.28000	Yes	Install the 876840v5.dlm patch	073.065.28000. 876840v5
3	073.060.055.34540	073.065. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.065.34540.905956v2
4	073.060.005.24600	073.065.24600	N/A	Upgrade to 073.060.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.065.34540.905956v2
5	073.060.035.24100 or 073.060.055.33800	073.065.24100 or 073.065.33800	N/A	Upgrade to 073.060.066.08210 or higher Patch is not needed	073.066.08210 or higher

For WorkCentre 5845/5855/5865/5875/5890
WorkCentre 5865i/5875i/5890i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.190.035.24100** or less	**073.195.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.195.24100** or less
2	073.190.035.28000	073.195.28000	Yes	Install the 876840v5.dlm patch	073.195.28000. 876840v5
3	073.190.055.34540	073.195. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.195.34540.905956v2
4	073.190.005.24600	073.195.24600	N/A	Upgrade to 073.190.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.195.34540.905956v2
5	073.190.035.24100 or 073.190.055.33800	073.195.24100 or 073.195.33800	N/A	Upgrade to 073.190.066.08210 or higher Patch is not needed	073.196.08210 or higher

For WorkCentre 5945/5955
WorkCentre 5945i/5955i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.091.035.24100** 1 or less	**073.095.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.095.24100** or less
2	073.091.035.28000	073.095.28000	Yes	Install the 876840v5.dlm patch	073.095.28000. 876840v5
3	073.091.055.34540	073.095. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.095.34540.905956v2
4	073.091.005.24600	073.095.24600	N/A	Upgrade to 073.091.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.095.34540.905956v2
5	073.091.035.24100 or 073.091.055.33800	073.095.24100 or 073.095.33800	N/A	Upgrade to 073.091.066.08210 or higher Patch is not needed	073.096.08210 or higher

For WorkCentre 6655/6655i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.110.035.24100** or less	**073.115.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.115.24100** or less
2	073.110.035.28000	073.115.28000	Yes	Install the 876840v5.dlm patch	073.115.28000. 876840v5
3	073.110.055.34540	073.115. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.115.34540.905956v2
4	073.110.005.24600	073.115.24600	N/A	Upgrade to 073.110.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.115.34540.905956v2
5	073.110.035.24100 or 073.110.055.33800	073.115.24100 or 073.115.33800	N/A	Upgrade to 073.110.066.08210 or higher Patch is not needed	073.116.08210 or higher

For WorkCentre 7220/7225
WorkCentre 7220i/7225i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.030.035.24100** or less	**073.035.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.035.24100** or less
2	073.030.035.28000	073.035.28000	Yes	Install the 876840v5.dlm patch	073.035.28000. 876840v5
3	073.303.055.34540	073.035. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.035.34540.905956v2
4	073.030.005.24600	073.035.24600	N/A	Upgrade to 073.030.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.03.34540.905956v2
5	073.030.035.24100 or 073.030.055.33800	073.035.24100 or 073.035.33800	N/A	Upgrade to 073.030.066.08210 or higher Patch is not needed	073.036.08210 or higher

For WorkCentre 7830/7835
WorkCentre 7830i/7835i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.010.035.24100** or less	**073.015.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.015.24100** or less
2	073.010.035.28000	073.015.28000	Yes	Install the 876840v5.dlm patch	073.015.28000. 876840v5
3	073.010.055.34540	073.015. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.015.34540.905956v2
4	073.010.005.24600	073.015.24600	N/A	Upgrade to 073.010.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.015.34540.905956v2
5	073.010.035.24100 or 073.010.055.33800	073.015.24100 or 073.015.33800	N/A	Upgrade to 073.010.066.08210 or higher Patch is not needed	073.016.08210 or higher

For WorkCentre 7845/7855
WorkCentre 7845i/7855i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.040.035.24100** or less	**073.045.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.045.24100** or less
2	073.040.035.28000	073.045.28000	Yes	Install the 876840v5.dlm patch	073.045.28000. 876840v5
3	073.040.055.34540	073.045. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.045.34540.905956v2
4	073.040.005.24600	073.045.24600	N/A	Upgrade to 073.040.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.045.34540.905956v2
5	073.040.035.24100 or 073.040.055.33800	073.045.24100 or 073.045.33800	N/A	Upgrade to 073.040.066.08210 or higher Patch is not needed	073.046.08210 or higher

For WorkCentre 7970/7970i

	If Your Software Version Is System SW	or Network Controller	Ready for Patch?	Next step:	Network Controller Will Now Show:
1	**073.200.035.24100** or less	**073.205.24100** or less	N/A	Patch is not needed; device is not affected by this vulnerability	**073.205.24100**
2	073.200.035.28000	073.205.28000	Yes	Install the 876840v5.dlm patch	073.205.28000. 876840v5
3	073.200.055.34540	073.205. 34540	N/A	See Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.205.34540.905956v2
4	073.200.005.24600	073.205.24600	N/A	Upgrade to 073.200.035.34540 Then see Security Bulletin XRX16-012 and install the 905956v2.dlm patch	073.205.34540.905956v2
5	073.200.035.24100 or 073.200.055.33800	073.205.24100 or 073.205.33800	N/A	Upgrade to 073.200.066.08210 or higher Patch is not needed	073.206.08210 or higher

Install the Patch

You must download this patch. The patch is packaged in a ZIP format. Download the applicable zip file from the URL provided and extract the contents to a convenient location on your desktop. Do not try to open the DLM file; the DLM file must be loaded on the MFD as is. Make sure that software upgrade is set to 'Enabled' on the device before attempting to install the patch.

Patch Installation Methods

This patch can and should be installed by the customer. There is 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.
- Use a USB drive to send an Upgrade / Patch file to the device.

For these patches it is recommended that the patch be installed using the Machine Software Upgrade Method.

Machine Software (Upgrade) Method

1) Open an Internet browser window, connect to the multifunction device by entering the device's IP address in the Address field in the format http://xx.xxx.xxx.xx and then press the **Enter** key on the keyboard.
2) Select the **Properties** tab. A Login screen may be displayed. Enter the System Administrator's User ID and Password and select Login, The3 default User ID is *admin* and the default password is *1111*.
3) Select **General Setup** and then select **Software Upgrade**.
   - If **Security Installation Policy: Not Allowed (Device and Remote methods)** is shown, the Software Upgrade option is disabled. Select the **Allow Upgrade** button. The pop-up message *Properties have been successfully modified* is displayed; select **OK**.
   - Set the **Security Installation Policy:** link and enable all options. This ensures that all the software upgrade functions are accessible. Select **Apply**. The pop-up message *Properties have been successfully modified* is displayed; select **OK.**
4) Select **Manual Upgrade**.
5) Select **Browse** button to locate and select the 876840v5.dlm file and select **Open**.
6) Select the **Install Software** button. The pop-up message *File has been submitted* is displayed. Select **OK**.

If you get a printed sheet with the message *This patch is not intended for this software version and was not installed*, ensure the device has software version 073.xxx.xxx.xxxxx installed.

When the software upgrade is complete, the device automatically reboots and prints a Software Upgrade Report and a new Configuration Report.

The patch is successfully installed when the Network Controller version shows 876840v5 appended to it.

Disclaimer