Security Bulletin XRX18-026
Xerox® "D"-Series Printers and Copier/Printers Address DLM Vulnerabilities

Bulletin Date: August 1, 2018

Update: November 8, 2018

Background

Vulnerabilities exist that, if exploited, could allow remote attackers to insert arbitrary code into the device. This could occur with a specifically crafted 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 all the network-connected releases[1] of the affected products listed below as follows:

1. Software upgrades can be disabled at the device by an administrator[2]:
    *   Xerox D95 Copier/Printer
    *   Xerox D95A Copier/Printer
    *   Xerox D110 Copier/Printer
    *   Xerox D125 Copier/Printer
    *   Xerox D136 Copier/Printer
    *   Xerox D110 Printer
    *   Xerox D125 Printer
    *   Xerox D136 Printer

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**.

[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.

Process to Disable Software Upgrades

Use the steps listed below for the indicated products on page 1 to disable software download on the device. Note that in each case only the System Administrator can perform these steps.
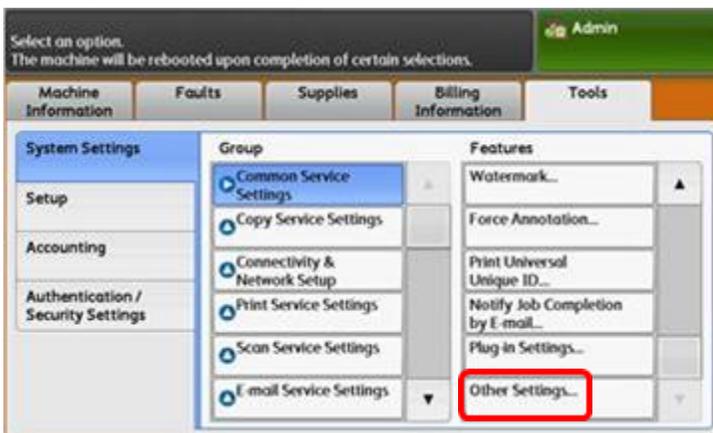
1. At your Control Panel (LUI), Press the physical login button and login as admin (admin,1111).

2. Once logged in press the physical **Machine Status** button which will bring you to following screen:
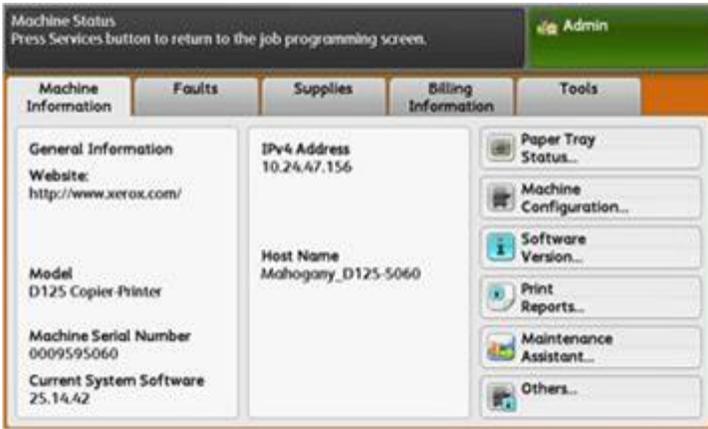
3. Navigate to **Tools** tab.

4. Select **System Settings->Common Service Settings** and scroll down on the **Features column** to access the **Other Settings** screen.

5. Once in the **Other Settings** screen scroll down to page 2, select the **Sofware Download** option and press the **Change Settings** button.
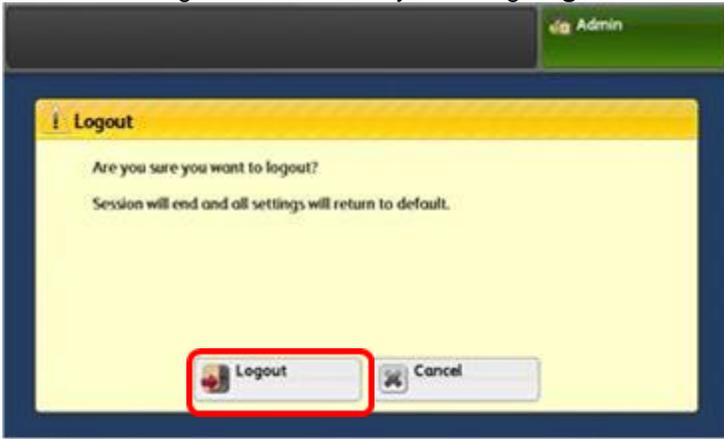

6. Set **Software Download** to disabled and **Save.**

7. On the following screen press the green **Admin** button located at the top right of the screen to pulldown the **Logout/Close Menu** option and select **Logout** option.

8. On the following screen confirm by selecting **Logout** button.

Software upgrades will now be disabled. If a software upgrade is planned to be performed, repeat these steps, set the **Enabled** option in step 6 and save, perform the software upgrade, then repeat the steps above to re-disable software upgrades