Security Bulletin XRX18-026

Xerox® “D”-Series Printers and Copier/Printers Address DLM Vulnerabilities

Bulletin Date: August 1, 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 upgrades on the device. Note that in each case only the System Administrator can perform these steps.

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 **Services** link.
6. Click on the **Machine Software** link.
7. Click on the **Upgrades** link.
8. Make sure the **Enabled** checkbox is not selected; if it is selected click on the checkbox to deselect it.
9. Click the **Apply** button.
10. Proceed to any other web page.

Software upgrades will now be disabled. If a software upgrade is planned to be performed, repeat these steps, checking the **Enabled** checkbox in step 8 instead of unchecking it, perform the software upgrade, then repeat the steps above to re-disable software upgrades.

Document Version: 1.0 (January 2017).