Mini Bulletin XRX16T
WorkCentre 3325
General Release 51.006.01.000

Release Date: Aug 26, 2016

Purpose

This Bulletin is intended ONLY for the specific security problems identified below. The problems identified has been rated a criticality level of **IMPORTANT.** This release includes OpenSSL 1.0.2d.

This is a general releases that incorporates fixes from previous SPAR releases as well as new fixes not included in previous releases. This general release includes fixes for:

- Fix for SSLv3 POODLE (Padding Oracle on Downgraded Legacy Encryption) vulnerability (CVE-2014-3566) – See Security Mini-Bulletin XRX15V
- Fix for CVE-2015-4000 Logjam Vulnerability in OpenSSL -- See Security Mini-Bulletin XRX15BA
- Fix for FREAK Vulnerability In OpenSSL (CVE-2015-0204) -- See Security Mini-Bulletin XRX15BA
- Fix for VxWorks TCP Sequence (CVE 2015-3963). Wind River VxWorks does not properly generate TCP initial sequence number (ISN) values, which makes it easier for remote attackers to spoof TCP sessions by predicting an ISN value.
- Security enhancements such as controlling machine access with IP Filtering, ability to require Admin credentials to print the configuration report, ability to restrict device web page access to admins only, ability to enable or disable the printing of configuration sheets at power on.

NOTE:
If the ‘Require SSLv3/TLS1.0 Enable’ checkbox is selected the device will support both SSLv3 and all versions of TLS, starting with TLS v1.2, then TLS v1.1, TLS v1.0 and SSLv3 in order.
If the ‘Only TLS Enable’ checkbox is selected the device will only support TLS Versions 1.2, 1.1 and 1.0, starting with TLS v1.2, then TLS v1.1 and then TLS v1.0.
If neither of the two checkboxes are selected the device will only support SSLv1 and SSLv2. **It is strongly recommended that one of the two checkboxes be selected.**

Software Release Details

If your software is higher or equal to the versions listed below no action is needed.

Otherwise, please review this bulletin and consider installation of this version.

Model	WorkCentre 3325
Firmware version	51.006.01.000
Link to update	Available here

Save the file to a convenient location on your workstation. Unzip the file if necessary.

Installation instructions:

Note: If authentication access control is enabled on the device, set the authentication method to No Authentication before attempting the upgrade.

Before starting the upgrade procedure, please ensure that the following items are available and/or the tasks have been performed:

1. The Software Upgrade file is obtained from the Xerox web site using the above link in this document. **IMPORTANT:** It is important to obtain the correct upgrade file for this device.
2. If you are performing the upgrade on a network connected machine, ensure that the machine is online before continuing. TCP/IP and HTTP protocols must be enabled on the machine so that the machine web browser can be accessed. Obtain the *IP Addresss* of the machine you want to upgrade.

<u>Manual Upgrade Using CentreWare Internet Services</u>

1. Open the web browser from your Workstation.
2. Enter the *IP Address* of the machine in the Address bar and select [**Enter**].
3. Login by clicking on the Login link at the top of the page and enter the Admin ID and Password.
4. Verify that the Firmware Upgrade is enabled:
    - Click on the [**Properties**] tab.
    - Click on the [**Security**] link on the left.
    - Click on the [**System Security**] link on the left.
    - Click on [**Feature Management**]
    - Click on the **Enable** checkbox for **Firmware Upgrade** and click **Apply**.
5. Click on [**Support**] tab.
6. Click on [**Firmware Upgrade**] on the left.
7. Click on the [**Upgrade Wizard**] button on the upper right hand corner.
8. The **Firmware Upgrade Wizard** screen appears. In the **Firmware File** area:
9. Select **Browse**.
10. Locate and select the software upgrade **.hd** file obtained earlier.
11. Select **Open**.
12. Select **Apply** to send the file to the machine.

<u>NOTES</u>

1. Please use ASCII characters only in the file path.
2. The file will be sent to the printer and will disable the printing functionality. The web browser will become inactive and you will not be able to access the machine via this method until the upgrade has completed and the machine has rebooted. The upgrade should take no longer than 30 minutes.
3. Once the machine has completed the upgrade it will reboot automatically. The configuration report will print (if enabled). Check the configuration report to verify that the software level has changed.