Mini Bulletin XRX16U
Phaser 3635MFP
General Release 20.106.02.000

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 XRX15W
- Fix for CVE-2015-4000 Logjam Vulnerability in OpenSSL -- See Security Mini-Bulletin XRX15AW
- Fix for FREAK Vulnerability In OpenSSL (CVE-2015-0204) -- See Security Mini-Bulletin XRX15W
- Fixes for security CVEs CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508 and CVE-2014-3510.
- Support for SHA384 cipher key issue- by fixing issue when customers are using Windows 2012 server and above. Windows 2012 server is choosing SHA384 cipher suite and during initial handshake itself server is sending a RESET. Since the issue is happening in openssl library debugging is very difficult so SHA384 was disabled.

NOTE:
If the ‘Require SSLv3 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 ‘TLS Only 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	**Phaser 3635MFP**
Firmware version	20.106.02.000
Link to update	Available here

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

Installation instructions:

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. The software upgrade file will have an '.hd' extension. **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.

Manual Upgrade Using CentreWare Internet Services

1. Open the web browser from your Workstation.
2. Enter the *IP Address* of the machine in the Address bar and select [**Enter**].
3. Verify that the Firmware Upgrade is enabled:
   - Click on the [**Properties**] tab.
   - Click on the [**Maintenance**] link.
   - Click on [**Upgrade Management**] link.
   - Click on [**Enabled**].
4. Click on [**Firmware Upgrade**].
5. In the **Firmware Upgrade** box click on **Browse** to locate and select the software upgrade **.hd** file obtained earlier.
6. Click on the **.hd** file.
7. Click on the [**Open**] button.
8. Click on the [**Install Software**] button to proceed with the upgrade. If prompted, enter the Administrator's User ID [**admin**] and Password and click on [**Login**]. .

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.

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.