# Mini Bulletin XRX16H
# WorkCentre 3025/3215/3225
# Phaser 3020/3052/3260
# General Release 3.50.01.13

**Bulletin Date: Mar 1, 2016**

## Purpose

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

Includes fixes for

- SSLv3.0 Poodle Vulnerability (CVE-2014-3566). SSLv3 supports an older encryption method that is no longer considered secure, and is no longer viable for protecting sensitive data in transmission over networks. This could allow a Man-in-The-Middle (MiTM) attack where a person on the network can force a “downgrade” of the session between a client and server to use SSLv3 instead of a more secure protocol such as TLS.

  Fixed by disabling SSL and using TLS only.
- FREAK Vulnerability in OpenSSL (CVE-2015-0204). A vulnerability in the OpenSSL library for SSL/TLS has been reported that can allow an attacker to execute a man-in-the-middle attack against vulnerable systems that support older key exchange methods. Xerox has included a non-vulnerable version of OpenSSL in the software version available below.

## 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 3052/3260 | Phaser 3020 | WorkCentre 3215/3225 | WorkCentre 3025BI | WorkCentre 3025NI |
|---|---|---|---|---|---|
| System SW version | 3.50.01.13 | 3.50.01.13 | 3.50.01.13 | 3.50.01.13 | 3.50.01.13 |
| Link to update | Available here | Available here | Available here | Available here | Available here |

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

## NOTE:

The "TLS Only" or "Only TLS" checkbox will be enabled by default and will support TLS versions 1.2, 1.1 and 1.0.

- When choosing the "TLS Only" or "Only TLS" checkbox, all SSL only connections will no longer work.
- When enabling the "Require SSL v3" option, the device will use SSLv3 only to establish a connection.

- The 2 features, "TLS Only" and "Require SSL v3" are mutually exclusive of one another, if one is checked the other must be unchecked. Also, if both features are off (unchecked), the device will use SSL (all versions) and TLS (all versions) simultaneously if needed

## The Installation Instructions are as follows:

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

1. The Software Upgrade file (Firmware file) is obtained from the Xerox web site. Click the link next to the model of your machine in the Software Release Details section above.
   **IMPORTANT:** It is important to obtain the correct upgrade file for your particular model of machine.
2. Completely unzip the file to a known location on your computer. Do not leave the file in the zip folder.
3. Print a Configuration Report. See the Xerox http://www.support.xerox.com/support/enus.html Support knowledge base for instructions for your particular model.
4. Ensure that the machine is online before continuing. TCP/IP and HTTP protocols must be enabled on the machine so that the machine's web page can be accessed. Obtain the *IP Address* of the machine you want to upgrade.

**Manual Upgrade Using Internet Services**

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 address of the machine you want to upgrade.

1. Open the web browser from your computer.
2. Enter the *IP Address* of the machine in the Address bar and select **Enter**.
3. If prompted, enter the Administrator User Name (admin) and Password, and select Login.
4. Select **Properties**.
5. In **Security** on the left hand side, select the **System Security** link.
6. Select the **Feature Management** link in the directory tree.
7. If it is unchecked, select the **Firmware Upgrade** Enable box.
8. Click **Apply** to save the changes.
9. Select the **Support** tab.
10. In the **Firmware Upgrade** link click the **Upgrade Wizard** button.
11. The **Firmware Upgrade Wizard** screen appears. In the Firmware File area:
    a. Select **Browse**.
    b. Locate and select the software upgrade file with the **.hd** extension unzipped earlier.
    c. Select **Open**.
12. Select [**Next**]. The firmware will now be verified and display information about the upgrade file.
13. Click [**Next**] to continue. The upgrade file should take less than 10 minutes unless there are network issues.
14. Once the machine has completed the upgrade it wil reboot automatically. The Configuration Report will print (if enabled). Compare the report to the one printed earlier to verify that the software level has changed.