Mini Bulletin XRX15AE
Phaser 3320
SMPR4 53.005.24.000

Release Date: Aug 17, 2015

Purpose

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

Includes fix 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. Xerox has disabled SSLv3 in the latest device 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 3320
Device SW version	053.005.24.000
Controller version	2.50.04.24
Link to update	Available here

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

IMPORTANT – Read before installing Firmware

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

- When choosing the "TLS only" 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 SSLv3" 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:

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 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 ewnter the Admin ID and Password.
4. Verify that the Firmeare Upgrade is enabled:
    a. Click on the [**Properties**] tab.
    b. Clink on the [**Security**] link on the left.
    c. Clink on the [**System Security**] link on the left.
    d. Clink on [**Feature Management**].
    e. Check the **Enable** checkbox for **Firmware Upgrade** and click **Apply**.
5. Click on the [**Support**] tab.
6. Click on [**Firmware Upgrade**] on the left.
7. Click on the [**Upgrade Wizard**] button on the upper right hand corner.
8. Locate and select the software upgrade file obtained earlier. The firmware file wil have an externsion **.hd**.
9. Click [**Next**]. The firmware will go through a firmware verification step.
10. Click [**Next**] to start the download process.

NOTES

1. Please use ASCII characters only in the file path.
2. Software Installation will begin several minutes after the software file has been submitted to the machine. Once Installation has begun all Internet Services from the machine wil be lost, including the Web User Interface. The installation process can be monitoted from the Local UI.

Once the download is complete, print a Configuration Report to verify the firmware version.