Mini Bulletin XRX15AK
Phaser 3635MFP
SPAR Release 20.105.52.000

Release Date: Sep 16, 2015

Purpose

This Bulletin is intended ONLY for the specific security problems 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 software version available below.
- 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 3300MFP
Device SW version	20.105.52.000
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” or “Only TLS” checkbox will be enabled by default and will support TLS versions 1.2, 1.1 and 10.

- 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 available here.

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