Mini Bulletin XRX15BA
WorkCentre 3325
SPAR Release 51.005.35.000

Release Date: Dec 29, 2015

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.

Includes fix for:

- Logjam Vulnerability in OpenSSL (CVE-2015-0400). A vulnerability in TLS protocol versions 1.2 and earlier allows man-in-the-middle attacks to occur against vulnerable systems that support older key exchange methods. Xerox has included a non-vulnerable version of OpenSSL in the software version available below.
- 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.
- 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.

Additionally, includes fix to add FIPS-certified SNMPv3/AES implementation.

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	51.005.35.000
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.

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. 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. Locate and select the software upgrade file obtained earlier. The firmware file will have an extension **.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 will be lost, including the Web User Interface.
3. Once the download is complete, print a Configuration Report to verify the firmware version.