Mini Bulletin XRX16AI
WorkCentre 3325
Release SMP5R1 51.006.15.000

Release Date: Nov 30, 2016   Updated: Dec 01, 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 1.1.0.

This SPAR release includes fix for:

- CVE-2016-2177 -- OpenSSL incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service.
- CVE-2016-2183 - The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, are vulnerable to a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
- CVE-2015-2808 Bar Mitzvah. The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values. RC4 has been disabled in this release.

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	51.006.15.000
Link to update	Available here

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

Technical Support Operations

Installation Instructions:

Manual upgrade using Internet Services

This section provides instructions to upgrade machine software over the network via **Xerox CentreWare Internet Services (CWIS)**.

Note: If authentication access control is enabled on the device, set the authentication method to No Authentication before attempting the upgrade.
(Properties > Security → Authentication → Authentication → Authentication Method)

Information Checklist
Before starting the 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 links earlier in this document.
   IMPORTANT: It is important to obtain the correct upgrade file for your particular model of machine.
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 address* of the machine you want to upgrade.

Procedure

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 Firmware Upgrade is enabled:
   a. Click on the **[Properties]** tab.
   b. Click on the **[Security]** link on the left
   c. Click on the **[System Security]** link on the left
   d. Click 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 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.

Note 1: Please use ASCII characters only in file path.

Note 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 this machine will be lost, including this Web User Interface.

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

Technical Support Operations