Mini Bulletin XRX17AE

Xerox® WorkCentre® 3325

General Release 51.007.00.000

Bulletin Date: September 28, 2017

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 software release has OpenSSL 1.1.0c.

This is a general release that incorporates fixes from previous SPAR releases as well as new fixes not included in previous releases. This general release includes fixes for:

- Multiple LibTiff CVEs
- ietf-IPv6 CVE-2016-10142 where an attacker can leverage the generation of IPv6 atomic fragments to trigger the use of fragmentation in an arbitrary IPv6 flow and can subsequently perform any type of fragmentation-based attack against legacy IPv6 nodes
- Removal of SSLv3 and inclusion of independent TLSv1.0, TLSv1.1 and TLS1.2 ‘Enable/Disable’ checkboxes
- Fix for OpenSSL Memory Leak CVE-2016-6304 that can cause a denial of service

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
System SW version	51.007.00.000
Link to Update	Available here

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

Firmware Installation Procedure

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.