Mini Bulletin XRX15AO
ColorQube 8570/8870
Firmware Release PS 4.76.0

Release Date: Oct 26, 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:

- CVE-2014-0076: The Montgomery ladder implementation in OpenSSL does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.
- CVE-2014-0221: The dtls1_get_message_fragment function in OpenSSL can allow remote attackers to cause a denial of service.
- CVE-2014-0224 (aka the "CCS Injection" vulnerability): OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information via a crafted TLS handshake.
- CVE-2014-3470: The ssl3_send_client_key_exchange function in OpenSSL, when an anonymous ECDH cipher suite is used, can allow remote attackers to cause a denial of service.
- Cross-Site Scripting vulnerability that can allow attackers to execute arbitrary code or take control of the device.
- Includes fix for the OpenSSL MiTM (Man in the Middle) Vulnerability (CVE-2014-0224). This vulnerability in OpenSSL allows a Man in the Middle attack. The attack requires both hosts to have a vulnerable version of OpenSSL.
- Heartbleed Vulnerability (CVE-2014-0160). A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.
- 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 added an option to disable SSLv3 in the software version available below. Disabling SSLv3 removes vulnerability to this CVE.

Xerox has included a non-vulnerable version of OpenSSL in the software version available below.

NOTE: Make sure that **Require SSL V3** in the HTTPS Web UI page is not checked (disabled) and that **TLS Only** is checked (enabled).

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(s)	ColorQube 8570/8870
Firmware	PS 4.76.0
Net Controller	4.3.90.10.14.2015
Link to update	Available here

Save the file to a convenient location on your workstation.

The Installation Instructions are as follows:

The downloaded firmware file must be completely unzipped before sending to the printer. Failure to do so can cause installation issues.

Using CentreWare Internet Services (Windows & Mac)

1. Open the web browser from your Workstation.
2. Enter the *IP Address* of the machine in the Address bar and then press **Enter**.
3. Click on the **Print** button.
4. Click on the "File Download" link in the list of options on the left side of the window.
5. Depending on the browser being used, click on the **Browse** or **Choose File** button, and then browse to select the unzipped firmware file to be downloaded to the device.
6. Click on the blue, square button to send the file to the printer.

Using FTP (Windows & Mac)

1. Open the command prompt (Windows) or Terminal window (Mac).
2. Type in "ftp xxx.xxx.xxx.xxx" where x characters represent the IP address of the device, and press **Enter**.
3. Press **Enter** at the prompt line that contai8nes "Name (xxx.xxx.xxx.xxx:user)".
4. Type in "put /location/of/file.ps" where the full file name and patch are entered. If you drag and drop the FW file you are sending into the window (after "put"), the full path and file name will populate automatically.
5. Press **Enter** and the file will be transferred to the printer over FTP.

Using the Xerox File Downloader Utility (Windows only)

Assumes the Xerox File Downloader Utility has already been downloaded and installed on the computer. The Xerox File Downloaded Utility can be found here.

1. From the computer, open the Xerox File Downloader Utility. By default, the utility is installed in the following location on the computer's hard drive: C:\File Downloader.
2. Select the required printer under "Select the printer" to spool the file to from the list below the pull-down menu.

3. Click on the **Browse** button, and then browse to and select the file to be downloaded to the printer from the “Select the file to send to the printer” section.
4. Click on the **Send** button to send the file to the printer.

Using a USB Connection (Mac only)

1. Firmware files can be downloaded to the device connected over USB by dragging the FW file to the print queue on an Apple Macintosh.

Installation Notes:

1. It is **imperative** that no print jobs be submitted to the device while the firmware code is being updated.
2. Do not interrupt the system once the download is in progress. Interruptions or loss of power may corrupt the firmware and render the system temporarily unavailable. A service repair may be required to return the system to a working condition.
3. Some of the device’s settings may be changed from their present value back to the factory default values by the firmware update. It is recommended that customers print a new configuration page, save it, and use as a reference to restore the device’s settings after the firmware update is complete.