Mini Bulletin XRX17G

Xerox® Phaser® 7800

SPAR Release R17-04 081.150.107.11800

Bulletin Date: May 16, 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 release includes OpenSSL 1.0.2j.

Includes fix for the following vulnerabilities:

- Mitigations for CVEs in multiple components that could result in DoS attacks (CVE-2016-6304, CVE-2016-6306, CVE-2014-0236, CVE-2016, CVE-2016-6303, CVE-2016-2179, CVE-2016-2181, CVE-2016-6302, CVE-2015-8710, CVE-2016-4447, CVE-2016-4449, CVE-2016-2109, CVE-2016-2105, CVE-2016-2106, CVE-2016-2177)
- CVE-2015-8540 -- Integer underflow in the png_check_keyword function in pngwutil.c in libpng allows remote attackers to have unspecified impact via a space character as a keyword in a PNG image
- CVE-2015-4642 -- The escapeshellarg function in ext/standard/exec.c in PHP allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function
- CVE-2016-4448 -- Format string vulnerability in libxml2 allows attackers to have unspecified impact via format string specifiers in unknown vectors
- CVE-2016-2108 -- The ASN.1 implementation in OpenSSL allows remote attackers to execute arbitrary code via an ANY field in crafted serialized data, aka the "negative zero" issue
- CVE-2016-2176 -- The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL allows remote attackers to obtain sensitive information from process stack memory
- CVE-2016-2107 -- The AES-NI implementation in OpenSSL does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.
- CVE-2016-2183 -- The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via 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-2016-9533 -- tif_pixarlog.c in libtiff has out-of-bounds write vulnerabilities in heap allocated buffers
- CVE-2016-9535 -- tif_predict.h and tif_predict.c in libtiff have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode

- CVE-2016-2178 -- The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack

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 7800
System SW version	081.150.107.11800
Link to update	Available here

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

Installation instructions:

Do not interrupt system once download is in process. Interruptions or loss of power may corrupt the engine firmware and render the system temporary unusable. (Service repair may be required to return the system to a working condition.)

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 customers save the configuration page and use it as a reference to restore the device's settings after the firmware update is complete.

Updating the Software over a Network Connection:
To download a file to the device using CentreWare Internet Services (Windows and Mac):
NOTE: CWIS can only be accessed if the device is connected to a network that utilizes the TCP/IP protocol. The device must also contain a valid IP Address.

1. From a computer, open an Internet web browser.
2. Enter the Phaser device's IP Address in the Address field, and then press Enter.
3. Click on the Properties tab. You may be prompted to login. Default account = 'admin', password = '1111'.
4. Click General Setup | Machine Software | Upgrades in the list of options on the left side of the window and verify that Enabled is checked. If it is not, check it and click on the Apply button.
5. Click Manual Upgrades in the list of options on the left side of the window.
6. Depending on the browser being used, click the Browse button, and then browse to and select the Phaser_7800_system-sw#08115010628600#.DLM file.
7. Click the Install Software button to send the file to the device.

The browser will display a dialog once the file has been transferred to the device. A progress indicator is displayed on the front panel. Upon completion, the device will reboot.