Mini Bulletin XRX16Y
Phaser 6360
SPAR Release 5.1.14

Release Date: Sep 2, 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 is a general releases that incorporates fixes from previous SPAR releases as well as new fixes not included in previous releases. This general release includes fixes for:

- SSLv3 POODLE (Padding Oracle on Downgraded Legacy Encryption) 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.
- MiTM-OpenSSL (CVE-2014-0224) where 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.
- Cross-Site Scripting Vulnerability.

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 6360
Firmware version	5.1.14
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 FW over a network connection

To download a file to the device using FTP (Windows and Mac):

NOTE: To perform this solution, the device must be connected to a network that utilizes the TCP/IP protocol. The device must also contain a valid IP Address.

1. Open the Command Prompt (Windows) or Terminal window (Mac).
2. Type in "ftp xxx.xxx.xxx.xxx", where the x characters represent the IP Address of the device, and press Enter.
3. Press Enter at the prompt line that contains "Name (xxx.xxx.xxx.xxx:user):"
4. Type in "put /location/of/file.ps", where the full file name and path 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.
5. Press Enter and the file will be transferred to the Phaser device over FTP.

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 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 and select the file to be downloaded to the device.
6. Click on the blue, square button to send the file to the Phaser device.