

Mini Bulletin XRX16AK Phaser 3300MFP SPAR Release 1.50.00.23 SMP2R5

Release Date: Dec 08, 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 1.1.1.0.

This SPAR release includes fix for:

- Introduce support for 1024 bit certificate key length. 512 bit key length is no longer supported
- 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 | Phaser 3300MFP |
|---------------------------|--------------------------------|
| Firmware version | 1.50.00.23 |
| Link to update | Available here |
| Installation Instructions | Available here |

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

Note:

1. Please ensure that you have a copy of your certificates prior to performing this upgrade since the upgrade will delete installed certificates.
2. If your certificate is of a key length less than 1024 bits it cannot be installed on this system after the upgrade.