

Mini Bulletin XR16K

WorkCentre 7755/7765/7775

SPAR Release 061.090.226.05000

Bulletin Date: Mar 18, 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 0.9.8zg.

Includes fix for:

- CVE-2015-4000 Logjam Vulnerability in OpenSSL: A vulnerability in TLS protocol versions 1.2 and earlier allows man-in-the-middle attacks to occur against vulnerable systems that support older key exchange methods. Xerox has included a non-vulnerable version of OpenSSL in the software version in this release.
- 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, aka the "Bar Mitzvah" issue. 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	Workcentre 7755/7765/7775
Firmware version	061.090.226.05000
Link to Software Release	Available here
Link to Installation Instructions	Available here

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