

Mini Bulletin XR15AR

WorkCentre 4250

SPAR Release 15.005.40.000

Release Date: Oct 1, 2015



Purpose

This Bulletin is intended **ONLY** for the specific security problem identified below. The problem identified has been rated a criticality level of **IMPORTANT**

Includes fix for:

- 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.
- Logjam Vulnerability In OpenSSL (CVE-2015-0400). 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 available below.
- Fix for TCP vulnerability in VxWorks.

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 4250
System SW version	15.005.40.000
Link to update	Available here

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

The Installation Instructions are [Available here](#).