Mini Bulletin XRX15AJ
WorkCentre 3550
SPAR Release 25.003.33.000

Release Date: Sep 9, 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 disabled SSLv3 in the software version available below.
- FREAK Vulnerability In OpenSSL (CVE-2015-0204). A vulnerability in the OpenSSL library for SSL/TLS has been reported that can allow an attacker to execute a man-in-the-middle attack against vulnerable systems that support older key exchange methods. Xerox has included a non-vulnerable version of OpenSSL in the software version available below.

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 3550
System SW version	25.003.33.000
Main Controller version	1.03.33.00
Network Controller version	4.02.02.13
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.

Technical Support Operations