Internal Release Notes
WorkCentre® 4260
General Release 30.107.01.000-SMP5

Release Date: September 21, 2017 **dc17rn3663**

Software Release Details

System Software	Version
Firmware	30.107.01.000
MCB	2.50.07.01
Engine (IOT)	0.41.69
Network	4.03.12

IMPORTANT: Once this digitally signed release is installed, the machine CANNOT be downgraded to a non-digitally signed release. Releases less than v30.105.05.000 are NOT digitally signed.

Purpose

This firmware release contains fixes and features added since version 30.103.33.000:

- Security - Remove 3DES from Embedded Web Server Available Ciphers List
- Security - Nexpose v6.4.14 SSL/TLS Security Alignment
- Security - ietf-IPv6 CVEs: CVE-2016-10142
- Security - LibTiff CVEs [SEC SB16-333,SB17-030]
- Security - Device is vulnerable to SWEET32 attack due to the presence of IDEA cipher in cipher list.
- SEC SB16-179 Vulnerability - OpenSSL Undefined Pointer Arithmetic
- LDAP Lookups Fail After Upgrading to 30.106.00.000

I. Installation Instructions

Software and installation instructions are available from http://www.xrxgsn.com/admin/user/general_release.ihtml
For details on how to upgrade your device, please see the System Administrator Guide

II. Problems Fixed

Log #	SFR / SPAR #	OPCO	Eureka #	Description
	CQGbl01142423	NA		Security - Remove 3DES from Embedded Web Server Available Ciphers List
NA 157357755 109316548 608549003	CQGbl01142420 CQGbl01081182 CQGbl01081179 CQGbl01081186	NA US-WVDS US-WVDS US-WVDS	NA NA NA NA	Security - Nexpose v6.4.14 SSL/TLS Security Alignment

Log #	SFR / SPAR #	OPCO	Eureka #	Description
NA	CQGbl01142408	NA	NA	Security - ietf-IPv6 CVEs: CVE-2016-10142
	CQGbl01142391			Security - LibTiff CVEs [SEC SB16-333,SB17-030]
	CQGbl01164043			Security - Device is vulnerable to SWEET32 attack due to the presence of IDEA cipher in cipher list.

III. Problems Fixed Since SPAR Release 30.105.26.000

Log #	SFR / SPAR #	Version	Eureka #	Description
264419879	1085549	30.106.11.000	1388575	LDAP Lookups Fail After Upgrading to 30.106.00.000
NA	Xerox Internal	30.106.10.000	NA	SEC SB16-179 Vulnerability - OpenSSL Undefined Pointer Arithmetic
21436449	989393	30.105.42.000	1381368	Unable to Scan to Email using Gmail account
66398	869312	30.105.42.000	1373907	Secure LDAP fails when negotiated cipher suite is SHA-384
NA	NA	30.105.41.000	NA	Security: Security Vulnerability- LOGJAM vulnerability + TCP Vulnerability in VxWorks
20524666	756493	30.105.40.000	1352445	Font Format is Incorrect When PCL Macro is Saved to HD vs RAM
63501	756917	30.105.40.000	1352444	Set LDAP ssl enabled via CWW or XDM does not apply to machine
63062	713171	30.105.39.000	1352430	Machine admin password doesn't work with upper case letters set by CWWeb or Device WebPage. Works OK with CAPS on Local UI.
NA	303367	30.105.39.000	NA	303367 Support Scan to Home with Domain.
20196778	671865	30.105.37.000	NA	This Model is Flushing some Print Jobs, while other similar Print Jobs print just fine.
57344	621234	30.105.37.000	1332010	DHCP leasing behavior incorrect.
NA	679001	30.105.37.000	NA	Security- This FW includes mitigation of the Poodle and Freak vulnerability by implementing a change to default SSL to off and use TLS only. The "TLS Only" or "Only TLS" checkbox will be enabled by default and will support TLS versions 1.2, 1.1 and 1.0. When choosing the "TLS Only" or "Only TLS" checkbox, all SSL only connections will no longer work. If “TLS Only” or “Only TLS” is unchecked, the device will use SSL (v1 or v2) and TLS (all versions) simultaneously if needed.
60525	638654	30.105.36.000	NA	LDAP Username Password visible in HTML source code.
NA	NA	30.105.35.000	NA	OpenSSL vulnerability fix also known as ‘man-in-the-middle’ (MiTM).
56169	541084	30.105.34.000	1305386	Device sends requests to dcs.support.xerox.com with Smart eSolutions disabled.
58069	587579	30.105.34.000	1312325	Authentication with umlaute/special characters in password do not work (Euro symbol).
58069	587579	30.105.31.000	1312325	Authentication with umlaute/special characters in password doesn't work.
19677605	569042	30.105.30.000	1309503	Scan to Email fails to outbound.att.net.
54804	512998	30.105.29.000	1302158	Scan to home fails when ports 137 and 139 (NetBIOS) are disabled on the server or switch.
38628	187833	30.105.28.000	NA	When using build job and Scan to Email, printer reboots after 46 pages scanned.