Mini Bulletin XRX16Q
WorkCentre 3655/3655i58XX/58XXi 59XX/59XXi/6655/6655i/72XX/72XXi 78XX/78XXi/7970/7970i

R16-05 SPAR Release
073.xxx.086.15410

Release Date: June 27, 2016 Update: October 27, 2016

Version 1.1

Purpose

This Bulletin is intended ONLY for the specific security problem identified below. The problem identified has been rated a criticality level of IMPORTANT. This SPAR release uses OpenSSL version 1.0.2f.

Includes fixes for:

- Disabling TLS 1.0 security protocol embedded HTTPS server only. Note that TLS 1.0 is enabled by default on these devices.
- Unsafe File-Directory Permissions
- An OS Command Injection found in the configrui.php file.
- CVE-2015-7547. Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response.
- CVE-2014-9425, CVE-2014-9426, CVE-2015-7803, CVE-2015-7804, CVE-2015-5590, CVE-2015-6831, CVE-2015-6832, CVE-2015-6836. Multiple vulnerabilities in PHP (e.g., Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors) require an upgrade to PHP.
- CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317. Multiple vulnerabilities in libxml2 (e.g., Heap-based buffer overflow in the xmlDictComputeFastQKey function in dict.c in libxml2 allows context-dependent attackers to cause a denial of service via unspecified vectors) requires an upgrade to libxml2 version 2.9.3 or greater.
- CVE-2016-0701, CVE-2015-3194, CVE-2015-3195, CVE-2016-0701. Multiple vulnerabilities in OpenSSL (e.g., The DH_check_pub_key function in crypto/dh/dh_check.c in OpenSSL does not ensure that prime numbers are appropriate for Diffie-Hellman (DH) key exchange, which makes it easier for remote attackers to discover a private DH exponent by making multiple handshakes with a peer that chose an inappropriate number) requires an upgrade to PenSSL 1.0.2f.
- CVE-2015-5296. Samba supports connections that are encrypted but unsigned, which allows man-in-the-middle attackers to conduct encrypted-to-unencrypted downgrade attacks by modifying the client-server data string.

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 3655/3655i	WorkCentre 58XX[1]/58XXi[2]	WorkCentre 59XX/59XXi[3]	WorkCentre 6655/6655i
System SW version	073.060.086.15410	073.190.086.15410	073.091.086.15410	073.110.086.15410
Network Controller version	073.066.15410	073.196.15410	073.096.15410	073.116.15410
Link to SW update and Install Instr.	Available here	Available here	Available here	Available here

Model	WorkCentre 72XX/72XXi[4]	WorkCentre 78XX/78XXi[5]	WorkCentre 78XX/78XXi[6]	WorkCentre 7970/7970i
System SW version	073.030.086.15410	073.010.086.15410	073.040.086.15410	073.200.086.15410
Network Controller version	073.036.15410	073.016.15410	073.046.15410	073.206.15410
Link to SW update and Install Inst.	Available here	Available here	Available here	Available here

Unzip the file to a known location on your workstation/computer.

General Information

Upgrading to 073 release

The recommended method is to use the Automatic Upgrade tool, also known as Software Upgrade Utility

Automatic Upgrade Utility Error Messages

“A connection with the device has been lost. Restart the device and select continue…”. Check if PDL Switching is enabled on the Raw TCP/IP port (port 9100). By default, PDL Switching is disabled. To use the tool, disable PDL switching. After the upgrade, enable PDL
switching again. This will be fixed in a future SW Upgrade Tool version.

To disabled/enable PDL Switching: Go to the device web page, Properties>Connectivity>Setup>Raw TCP/IP Printing>Select Edit. If PDL Switching is enabled, select the box to remove the check mark. Select Apply.

A message “No supported device found using IP # or Hostname. Enter a valid IP address or hostname and try again.” Check if the device is using HTTPS. If it is, ensure you select the “Enable HTTPS” option on the software upgrade utility.

If you call support for an issue using the upgrade utility, ensure you provide the CKToolUpgradexxx.log file that coincides with the issue. This log file is located in the folder where you launched the tool.

[1] WorkCentre 5845/5855/5865/5875/5890
[2] WorkCentre 5865i/5875i/5890i
[3] WorkCentre 5945/5945i/5955/5955i
[4] WorkCentre 7220/7220i/7225/7225i
[5] WorkCentre 7830/7830i/7835/7835i
[6] WorkCentre 7845/7845i/7855/7855i

Manual Tool Upgrade
You must follow the instructions closely. Skipping steps and not using pre-upgrade patches in the correct order will result in lost settings and you will need to reconfigure your machine manually.

ConnectKey Software Version Information

The software version numbers have specific meaning. When comparing ConnectKey version numbers to determine older/newer
1) Ensure you only compare those that start with the same first three digits (073).
2) Then look at the last six digits only.

New General release: 073.xxx.07**5.34540** **- 5= 2015. 345=day 345 of the year. 40 is respin 4.**
New SPAR release: 073.xxx.06**6.08210** **- 6=2016. 082=day 82 of the year. 10 is respin 1.**

073…534540
073…608210
608210 is a higher number than 534540.
The fixes and features that will be in the 073…5.34540 (general release) are also in 073…6.08210 (SPAR Release)