Mini Bulletin XRX16L
WorkCentre 3655/3655i58XX/58XXi 59XX/59XXi/6655/6655i/72XX/72XXi 78XX/78XXi/7970/7970i
R16-02 SPAR Release
073.xxx.066.08210

Release Date: April 15, 2016

Version 1.0

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 1.0.1p.

Includes fixes for:

- Includes fix for CVE-2013-2566 and 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. RC4 has been disabled in this release.

- Includes fix for CVE-2011-3389 (BEAST): The SSL protocol encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API.

- Includes fix for CVE-2015-3183: The chunked transfer coding implementation in the Apache HTTP Server does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request.

- Includes fix for CVE-2015-3185: The ap_some_auth_required function in server/request.c in the Apache HTTP Server does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Includes fix for CVE-2015-8126: Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.

- Includes fix for CVE-2015-7981: The png_convert_to_rfc1123 function in png.c in libpng allows remote attackers to obtain sensitive process memory information via crafted tIME chunk data in an image file, which triggers an out-of-bounds read.

- Includes fix for CVE-2014-9751: The read_network_packet function in ntp_io.c in ntpd in NTP does not properly determine whether a source IP address is an IPv6 loopback address, which makes it easier for remote attackers to spoof restricted packets, and read or write to the runtime state, by leveraging the ability to reach the ntpd machine's network interface with a packet from the ::1 address.

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	073.060.066.08210	073.190.066.08210	073.091.066.08210	073.110.066.08210
Network Controller version	073.066.08210	073.196.08210	073.096.08210	073.116.08210
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	073.030.066.08210	073.010.066.08210	073.040.066.08210	073.200.066.08210
Network Controller version	073.036.08210	073.016.08210	073.046.08210	073.206.08210
Link to SW update and Install Inst.	Available here	Available here	Available here	Available here

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

Note: For the WorkCentre 3655 & WorkCentre 6655 Only: Once the system is upgraded to this SPAR release it cannor be downgraded to GM release 072.060.034.16800 / 072.111.044.20500, respectively, or SPAR release 072.060.134.32804 / 072.110.134.32804, respectively.

[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