Mini Security Bulletin XRX14A
WorkCentre 57xx Series
Release 061.132.224.08800

Release Date: May 20 2014

Version 1.0

Software Release Details

Component	Version
System Software	061.132.224.08800
Network Controller	061.134.08820
UI	028.071.00040
IOT Pre-Mod Tag Revision	093.071.000
IOT w/Mod Tag 155	095.038.000
SIP	028.080.00023
DADH	025.020.000
Net Controller OS	061.064.05000

Purpose

This Bulletin is ONLY intended for the specific security problem(s) identified below. The problem(s) identified has been rated as **critical**.

- CVE-2011-3192 - The byterange filter in the Apache HTTP Server allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges.
- CVE-2012-0053 - protocol.c in the Apache HTTP Server allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.
- CVE-2011-3188 the Linux kernel makes it easier for remote attackers to cause a denial of service (disrupted networking) or hijack network sessions by predicting these values and sending crafted packets.
- CVE-2011-4885 - PHP allows remote attackers to execute arbitrary code via a request containing a large number of variables, related to improper handling of array variables.
- CVE-2012-1182 – In the The RPC code generator in Samba allows remote attackers to execute arbitrary code via a crafted RPC call.

- CVE-2010-2063 – The process.c in smbd in Samba allows remote attackers to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a crafted field in a packet.
- CVE-2011-0719 - Samba allows remote attackers to cause a denial of service (stack memory corruption, and infinite loop or daemon crash) by opening a large number of files, related to (1) Winbind or (2) smbd.
- CVE-2012-0870 - In process.c in smbd in Samba allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code
- Multiple PHP CVEs

Installation Notes

Firmware Release File

Release Install File	061.132.224.08800 or greater contain these fixes

The SPAR Software is located here. Save the files to a convenient location on your workstation. Unzip the file if necessary.

Installation Notes

When upgrading to **61.132.222.03800** or later from any release less than **61.132.222.03800**, pre-upgrade patch **361374v1.dlm** (found in the .zip file) may need to be installed before upgrading to this latest release. The pre-upgrade patch will retain the **Default Scan Template** settings that were made prior to loading **61.132.222.03800**. If you upgrade to **61.132.222.03800** or later without loading the pre-upgrade patch first, the **Default Scan Template** settings will reset back to factory default at which point you will need to manually set the **Default Scan Template** to the desired settings.

361374v1.dlm

If a machine has the engineering version 61.130.220.33700 installed, you m**ust** install the following pre-upgrade patch(CQ286115v1) BEFORE upgrading to the new release. If you have **any other version**, you **do not need** this (CQ286115v1) pre-upgrade patch. Install the patch using the Machine Upgrade web page process. Open the zip file and then extract the patch.

SW upgrade patch for 33700 release.zip