Overview

This document describes a patch that addresses two known Apache Struts2 vulnerabilities. This patch is designed to address these specific Struts2 vulnerability issues and updates Struts2 in CPPM to version 2.3.15.1.

What's included in the patch?

This ClearPass patch update contains security updates for the following:
- CVE-2013-2251: The vulnerability could be introduced by manipulating parameters prefixed with "redirect:"/"redirectAction:", which would allow open redirects.

- CVE-2013-2248: The vulnerability could be introduced by manipulating parameters prefixed with "action:"/"redirect:"/"redirectAction:", which would allow remote command execution.

Where can I get the patch?

This patch is available for ClearPass Policy Manager (CPPM) versions 6.1.x and 6.2. The patch is available in the CPPM UI on the **Administration > Agents and Software Updates > Software Updates** page. If you are not signed up for live updates, or if you want to perform an offline install, the patch is also available for download on the Aruba Networks support site at http://support.arubanetworks.com.

- For 6.2, download the **6.2 Struts vulnerability patch** file, (filename **CPPM-x86_64-20130801-struts-vulnerability-fix-patch.zip.signed)**, at downloads/ClearPass/PolicyManager/CurrentRelease/Patches

- For 6.1.x, download the ClearPass 6.1 Cumulative Patch 3 at downloads/ClearPass/PolicyManager/Archives/6.1.0/Patches

How do I install the patch that I received offline?

Note: For the following download and import steps, there is a known issue with the Internet Explorer (IE) browser. Please use either the Firefox or Chrome browsers; do not use IE.
1. Download the patch from the Support site.
2. In CPPM, go to **Administration > Agents and Software Updates > Software Updates**.
3. In the **Firmware and Patch Updates** area, click **Import Updates** and browse to the patch file.

4. After importing it, you have two options for installing it:
   - Install through the ClearPass UI: This option is only available in ClearPass 6.2 and later versions. After importing the patch file, it is included in the list of available firmware updates. Click the
   Install button for the patch.

   - Install through the CLI: You can install through the CLI using the command.

system update -i [patchfilename]

Final Steps

After you install the patch, the Admin server will restart and you will need to log in to CPPM again.

- For 6.2, the CPPM version will change from 6.2.0.54353 to 6.2.0.54567.
- For 6.1.x, the CPPM version will change to 6.1.3.54640.

Alcatel-Lucent Service & Support

OBTAINING FIXED FIRMWARE
Alcatel-Lucent customers can obtain the firmware on the Aruba support website:
http://support.arubanetworks.com

Our Commitment to Enhancing Security
The Alcatel-Lucent OmniAccess WLAN products are distributed in cooperation with Aruba Networks. Alcatel-Lucent will continue to work closely with Aruba Networks in order to continuously enhance the security capabilities of the OAW products. Alcatel-Lucent will continue to work with its partner to address these issues and communicate the latest updates.

If you have any additional questions please feel free to contact us at
esd.support@alcatel-lucent.com.

North America Service and Support: 1-800-995-2696
Latin America Service and Support: 1-877-919-9526
EMEA: +800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific Service and Support: +65-6240-8484