Read Me:
ClearPass 6.1.4 & 6.2.6 Vulnerability Issues Patch, May 9, 2014

This patch addresses four security known issues, described in the Resolved Issues section. To resolve these issues, please apply the following patch: **ClearPass fixes for Struts security vulnerabilities - CVE-2014-0094, CVE-2014-0050, CVE-2014-0112, CVE-2014-0113**
This patch is available for the following releases:

- ClearPass 6.1.4
- ClearPass 6.2.6

Installation Instructions

Table 1 *ClearPass versions and patch filenames*

W-ClearPass Version	Filename
6.1.4	CPPM-x86_64-20140428-struts-security-fix-patch.zip.signed
6.2.6	CPPM-x86_64-20140428-struts-security-fix-62-patch.zip.signed

For ClearPass 6.1.4:

Before you apply this patch, your ClearPass version must be updated to 6.1.4.55458.
This patch can also be installed over 6.1.4.61696 (security fixes version), or 6.1.4.61038 (updates portal fixes), or 6.1.4.55486.

- If access is allowed to the Web service, CPPM servers will show the **ClearPass fixes for Struts security vulnerabilities - CVE-2014-0094, CVE-2014-0050, CVE-2014-0112, CVE-2014-0113** patch at **Administration > Agents and Software Updates > Software Updates**. Install the patch directly through the UI.
- Alternatively, for an offline update, you can download the patch from the support site, upload it to the CPPM server, and then install it using the UI or CLI. Use the signed patch from the support site: **CPPM-x86_64-20140428-struts-security-fix-patch.zip.signed**.
    - Upload this file to CPPM through the UI, and install it using the CLI (appadmin SSH access).
    - Run the following command to install the patch:
      system update -i CPPM-x86_64-20140428-struts-security-fix-patch.bin

For ClearPass 6.2.6:

Before you apply this patch, your ClearPass version must be updated to 6.2.6.62196.

- If access is allowed to the Web service, CPPM servers running 6.2.6 will show the **ClearPass fixes for Struts security vulnerabilities - CVE-2014-0094, CVE-2014-0050, CVE-2014-0112, CVE-2014-0113** patch at **Administration > Agents and Software Updates > Software Updates**. Install the patch directly through the UI.
- Alternatively, for an offline update, you may download the signed patch from the Support site, upload it to the CPPM server, and then install it through the UI.

Installing the Patch Online

To install the patch online through the Software Updates portal:

1. In CPPM, go to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware and Patch Updates** area, find the **ClearPass fixes for Struts security vulnerabilities - CVE-2014-0094, CVE-2014-0050, CVE-2014-0112, CVE-2014-0113** patch and click the **Download** button in its row.
3. After the patch is downloaded, click **Install**. When the installation is complete, if the status is shown as **Needs Restart**, restart ClearPass. The status for the patch is then shown as Installed. The version number is not changed after this patch installation.

Offline Update

To install the patch offline if ClearPass is not connected to the online Software Updates portal:

1. Download the appropriate **ClearPass fixes for Struts security vulnerabilities - CVE-2014-0094, CVE-2014-0050, CVE-2014-0112, CVE-2014-0113** patch from the support site (http://support.arubanetworks.com).
2. At the bottom of the **Firmware and Patch Updates** area, click **Import Updates** and browse to the downloaded patch file.
3. Click **Install**. When the installation is complete, if the status is shown as **Needs Restart**, restart ClearPass. The status for the patch is then shown as Installed. The version number is not changed after this patch installation.

Resolved Issues

Table 1 *Issues Fixed in this Patch*

Bug ID	Description
23368	Apache Struts2 is upgraded to the latest version to fix the following vulnerability known issues in Struts2: • CVE-2014-0094 - Apache Struts Zero-Day Exploit and Mitigation. For more information, see http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0094. • CVE-2014-0050 - Apache Commons FileUpload and Apache Tomcat Denial-of-Service. For more information, see http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0050. • CVE-2014-0112 - Incomplete fix for ClassLoader manipulation via ParametersInterceptor. For more information, see http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0112. • CVE-2014-0113 - ClassLoader manipulation via CookieInterceptor when configured to accept all cookies. For more information, see http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0113.