Read Me: ClearPass OpenSSL Vulnerability Issue Patch, April 9, 2014

This patch addresses the OpenSSL 1.0.1 Library vulnerability known issue, also known as the "Heartbleed bug." This patch is available for ClearPass 6.1.0 – 6.1.4, 6.2.6, and 6.3.1. To address this issue, first review the version information provided in the Installation Instructions section of this document. After you have reviewed the instructions, please apply the appropriate version of the patch:
ClearPass OpenSSL fix - Security Advisory CVE-2014-0160

Table 1 *ClearPass versions and patch filenames*

ClearPass Version	Filename
6.1.0, 6.1.1, and 6.1.2	CPPM-x86_64-20140408-61461696-openssl-fix-patch.bin
6.1.3 and 6.1.4	CPPM-x86_64-20140408-61461696-openssl-fix-patch.zip.signed
6.2.6	CPPM-x86_64-20140408-626-openssl-fix-patch.zip.signed
6.3.1	CPPM-x86_64-20140408-631-openssl-fix-patch.zip.signed

Note: After you install the patch and reboot, the status "Reboot of server initiated" is correctly shown at the top of the page, but the "Install in progress" indicator is also displayed. The indicator is incorrect and can be ignored, as the installation was completed before the reboot was initiated.

Description

A very serious vulnerability was discovered in the OpenSSL 1.0.1 library. This vulnerability is also known as the Heartbleed bug, and was announced through CVE-2014-0160. The vulnerability can allow an external attacker to extract segments of memory from a remote system without leaving any traces. This memory could contain vital security information, including private keys. These keys, in turn, could be used to mount a man-in-the-middle attack.

OpenSSL is a very widely used library, and this vulnerability is likely to affect many systems and Web sites. Aruba Networks uses this library in different products to secure communications between our infrastructure and various clients. This bug is in OpenSSL's implementation of the TLS/DTLS (transport layer security protocols) heartbeat extension (RFC6520). When exploited it leads to the leak from the server to the client. In some cases it has been demonstrated that key material may be part of this memory leak.

This issue affects ClearPass 6.1.0 – 6.1.4, 6.2.0 – 6.2.6, and 6.3.0 – 6.3.1. Earlier versions of ClearPass used an earlier version of OpenSSL that was not vulnerable. Aruba Central, Aruba Network's cloud-based Wi-Fi offering, upgraded their Web infrastructure to the latest and safe version of OpenSSL on April 7 after the attack was first published.

For more information, an Aruba Security Advisory for this issue is available at http://www.arubanetworks.com/support/alerts/aid-040814.asc. It provides additional details and describes affected Aruba products, mitigation steps, and how to obtain firmware that includes the fix.

Installation Instructions

NOTE: Because there is a chance that key material might already have been compromised, we further advise you to consider replacing your certificates after the update is completed. You should then reissue your client certificates.

Information for 6.1.x Customers:

- For 6.1, you can apply the 6.1 OpenSSL patch on any version from 6.1.0 through 6.1.4.
- If access is allowed to the Web service, CPPM servers will show the OpenSSL signed 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 Support site, upload it to the CPPM server, and then install it using the UI or CLI. **This is version-specific**, as follows:
    - Versions 6.1.0, 6.1.1, and 6.1.2 do not support signed patches. For these versions, please use the unsigned patch from the Support site:
      CPPM-x86_64-20140408-61461696-openssl-fix-patch.bin
      For these versions, upload the unsigned patch to CPPM through the UI and install using the CLI (appadmin SSH access).
    - Versions 6.1.3 and 6.1.4 support signed patches. Use the signed patch from the Support site:
      CPPM-x86_64-20140408-61461696-openssl-fix-patch.zip.signed
      Upload it 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_64-20140217-cppm-security-fix-patch.bin

Information for 6.2.x Customers:

- For 6.2, you must apply the 6.2 OpenSSL patch on the 6.2.6 cumulative patch. This is because 6.2.5 and 6.2.6 included another OpenSSL fix. If you are running any version of 6.2 older than 6.2.6, you must first update to 6.2.6 before applying this patch.
- If access is allowed to the Web service, CPPM servers running 6.2.6 will show the **ClearPass OpenSSL fix - Security Advisory CVE-2014-0160** patch at **Administration > Agents and Software Updates > Software Updates**. Install the patch directly through the UI.
- Alternatively, you may download the signed patch from the Support site, upload it to the CPPM server, and then install it through the UI.

Information for 6.3.x Customer:

- For 6.3, you must apply the 6.3 OpenSSL patch on the 6.3.1 cumulative patch. This is because 6.3.1 included another OpenSSL fix. If you are running 6.3.0, you must first update to 6.3.1 before applying this patch.

- If access is allowed to the Web service, CPPM servers running 6.3.1 will show the **ClearPass OpenSSL fix - Security Advisory CVE-2014-0160** patch at **Administration > Agents and Software Updates > Software Updates**. Install the patch directly through the UI.
- Alternatively, 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 portal:

1. In CPPM, go to **Administration > Agents and Software Updates > Software Updates**.
2. In the **Firmware and Patch Updates** area, find the **ClearPass OpenSSL fix - Security Advisory CVE-2014-0160** patch and click the **Download** button in its row.
3. For versions later than 6.1.4, 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**.

Offline Update

To install the patch offline if ClearPass is not connected to the cloud:

1. Download the appropriate **ClearPass OpenSSL fix - Security Advisory CVE-2014-0160** patch from the Support site.
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**.
4. For versions 6.1.0 through 6.1.4, after uploading the patch, log in to the CLI as the user **appadmin**.
   Run the following command to install the patch:
   system update –i CPPM-x86_64-20140408-61461696-openssl-fix-patch.bin
   After the installation has completed, enter the following command:
   system restart

Resolved Issues

Table 1 *Issues Fixed in this Patch*

Bug ID	Description
22949	Corrected the OpenSSL Vulnerability known as the Heartbleed bug (CVE-2014-0160). Additional information is available at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160.