Read Me: ClearPass OpenSSL Vulnerability Issue Patch, June 13, 2014

This patch addresses the OpenSSL vulnerability known issue described in CVE-2014-0224. This issue affects ClearPass 6.1.0 – 6.1.4, 6.2.0 – 6.2.6, and 6.3.0 – 6.3.3. The patch is available for ClearPass 6.1.0 – 6.1.4, 6.2.6, and 6.3.3. 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 for vulnerability - CVE-2014-0224

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

Multiple vulnerabilities were discovered in OpenSSL and announced on June 5, 2014. This ReadMe discusses the SSL/TLS MITM vulnerability described in CVE-2014-0224, which is the only one that affects ClearPass or other Aruba products.

This vulnerability can allow an attacker using a carefully crafted handshake to force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server. The attack can only be performed between a vulnerable server and client (both server and client must be running a vulnerable version of OpenSSL).

Most common Web browsers do not make use of OpenSSL, and thus HTTPS connections between a browser and an affected Aruba device would not be impacted. The major exception is Chrome running on Android devices, which does use OpenSSL. Wireless EAP sessions might be impacted between an affected Aruba product and a client device that uses OpenSSL as part of its EAP stack. This primarily impacts UNIX-like operating systems which employ the open-source "wpa_supplicant" package when it is built and linked against OpenSSL. Android is reported to use wpa_supplicant to manage 802.1X sessions. Aruba has not yet confirmed that EAP is vulnerable, but based on preliminary analysis:

- EAP-TLS will not reveal credentials during an attack. EAP-TLS uses TLS for certificate verification, and does not actually communicate encrypted authentication messages over a TLS tunnel.
- EAP-PEAP might be vulnerable to credential exposure. The impact would be the exposure of an MSCHAPv2 hash to an attacker, who could then conduct an offline dictionary or brute-force attack against the password hash. The strength of the password will determine how successful the attack is.
- For any EAP type, the Pairwise Master Key (PMK) used to protect the resulting wireless session is based off the TLS master secret. If a man-in-the-middle attack successfully forces weak keying material to be used, the resulting PMK will be similarly weak.

Given the ability to conduct man-in-the-middle attacks over a wireless network, Aruba recommends caution when connecting vulnerable client devices to WPA2 networks until either the client or server has been patched for this vulnerability.

For more information, an Aruba Security Advisory for this issue is available at http://www.arubanetworks.com/support/alerts/aid-06062014.txt. It provides additional details and describes affected Aruba products, mitigation steps, and how to obtain firmware that includes the fix.

Installation Instructions

Table 1 *ClearPass versions and patch filenames*

ClearPass Version	Filename
6.1.0, 6.1.1, and 6.1.2	CPPM-x86_64-20140606-openssl-fix-patch.bin
6.1.3 and 6.1.4	CPPM-x86_64-20140606-openssl-fix-patch.signed.bin
6.2.6	CPPM-x86_64-20140606-openssl-fix-62-patch.signed.bin
6.3.3	CPPM-x86_64-20140606-openssl-fix-63-patch.signed.bin

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 the 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_64-20140606-openssl-fix-patch.bin
      For these versions, upload the unsigned patch to CPPM through the UI and install it 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_64-20140606-openssl-fix-patch.signed.bin
      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_64-20140606-openssl-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 other OpenSSL fixes. 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 for vulnerability - CVE-2014-0224** 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 6.3.3 cumulative patch. This is because 6.3.1 and 6.3.2 included other OpenSSL fixes. If you are running 6.3.0, you must first update to 6.3.3 before applying this patch.
- If access is allowed to the Web service, CPPM servers running 6.3.3 will show the **ClearPass OpenSSL fix for vulnerability - CVE-2014-0224** 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 for vulnerability - CVE-2014-0224** patch and click the **Download** button in its row.
3. For versions later than 6.1.4, click **Install**.
4. 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 for vulnerability - CVE-2014-0224** patch from the Support site.
2. Open W-ClearPass Policy Manager and go to **Administration > Agents and Software Updates > Software Updates**.
3. At the bottom of the **Firmware and Patch Updates** area, click **Import Updates** and browse to the downloaded patch file.
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**.
5. For versions 6.1.0 through 6.1.2, 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_64-20140606-openssl-fix-patch.bin
   After the installation has completed, enter the following command:
   system restart
6. For versions 6.1.3 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_64-20140606-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
#24082	Corrected the OpenSSL Vulnerability described in CVE-2014-0224. Additional information is available at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224.