# Read Me: GNU Bash Shell Vulnerability Issue Patch, October 1, 2014

This patch addresses the vulnerability known issue described in CVE-2014-6271 and CVE-2014-7169.

* This issue affects ClearPass 6.2.x and 6.3.x.
* The patch is available for all ClearPass 6.2.x and 6.3.x versions.
* The ClearPass 6.4.1 release includes the fix for 6.4.x.

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 vulnerability update for CVE-2014-6271, CVE-2014-7169**

**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

On September 24, 2014, a public announcement was made regarding a vulnerability in the GNU Bash shell that could permit remote code execution through environment variables. This vulnerability was assigned CVE-2014-6271 and fixes were published. The fix was incomplete, and a second vulnerability, CVE-2014-7169, was published. This ReadMe discusses this vulnerability.

The GNU Bash shell is third-party software. Bash supports exporting not just shell variables, but also shell functions to other Bash instances, via the process environment to (indirect) child processes. The vulnerability occurs because Bash does not stop after processing the function definition; it continues to parse and execute shell commands following the function definition. If Bash is used as an interpreter for network-accessible scripts, an attacker could exploit the vulnerability to execute arbitrary code.

Aruba confirms that affected versions of Bash are included in the Linux distribution used by ClearPass. After detailed analysis of how Bash is used, including where it may be used by third-party software components, we have determined that it is difficult to successfully exploit it, and have downgraded its CVS score to Low (3.6).

Aruba recommends that wherever possible, affected products should not be exposed to untrusted networks such as the public Internet. If you are using ClearPass 6.2.x or 6.3.x, we recommend that you apply the appropriate patch for your ClearPass version as soon as possible. If you are using a ClearPass version earlier than 6.2, you should upgrade to a later version as soon as is practical.

For more information, an Aruba Security Advisory for this issue is available at <http://www.arubanetworks.com/support/alerts/aid-09252014.txt> . It provides additional details and contact information.

## Installation Instructions

|  |  |
| --- | --- |
| **Table 1** *ClearPass versions and patch filenames* | |
| **ClearPass Version** | **Filename** |
| 6.2.0 through 6.2.6 | CPPM-x86\_64-20140925-bash-cve-2014-7169-fix-62-patch.signed.bin |
| 6.3.0 through 6.3.5 | CPPM-x86\_64-20140925-bash-cve-2014-7169-fix-63-patch.signed.bin |

### Information for 6.2.x Customers:

* If access is allowed to the Web service, CPPM servers running 6.2.x will show the   
  **ClearPass vulnerability update for CVE-2014-6271, CVE-2014-7169** 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:

* If access is allowed to the Web service, CPPM servers running 6.3.x will show the patch at **Administration > Agents and Software Updates > Software Updates**. Install the patch directly through the UI.
* Alternatively, you may download the patch from the Support site, upload it to the CPPM server, and then install it through the UI.
* Full update instructions are provided in the ClearPass 6.3.5 Release Notes.

### 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 vulnerability update for CVE-2014-6271, CVE-2014-7169** patch and click the **Download** button in its row.
3. 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 vulnerability update for CVE-2014-6271, CVE-2014-7169** 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**.

## Resolved Issues

|  |  |
| --- | --- |
| **Table 1** *Issues Fixed in this Patch* | |
| **Bug ID** | **Description** |
| #25831 #25855  #25858 #25859 | This patch includes fixes for CVE-2014-6271 and CVE-2014-7169, a Bash code injection vulnerability issue that could allow for arbitrary code execution through environment variables. Additional information is available at  <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271> and <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169>. |