Security Advisory on Critical Updates for Pivotal Command Center

April 21, 2014

Pivotal Security Advisory	
Synopsis:	Pivotal Command Center needs an update of the OpenSSL component
Issue date:	2014-04-21
Updated on:	2014-04-21
CVE	CVE-2014-0160

Topics

Copyright

Use of Open Source

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, Pivotal will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. Pivotal may charge reasonable shipping and handling charges for such distribution.

About Pivotal Software, Inc.

Greenplum transitioned to a new corporate identity (Pivotal, Inc.) in 2013. As a result of this transition, there will be some legacy instances of our former corporate identity (Greenplum) appearing in our products and documentation. If you have any questions or concerns, please do not hesitate to contact us through our web site: http://gopivotal.com/about-pivotal/support.

Summary

This advisory describes a *possible* need to perform a security update of the OpenSSL RPM in Red Hat Enterprise Linux and/or CentOS 6.x that is used by Pivotal Command Center (PCC). The security update should be applied immediately to fix the critical security vulnerability reported in CVE-2014-0160. The scope of this important vulnerability is described in http://www.kb.cert.org/vuls/id/720951.

Relevant Releases

This advisory applies to systems hosting the following releases:

- Pivotal Command Center 2.0.x
- Pivotal Command Center 2.1.x

Problem Description

On April 7th, 2014, an OpenSSL vulnerability was disclosed which has a critical security hole. The bug, called the Heartbleed bug, was introduced in OpenSSL version 1.0.1. It has been patched with OpenSSL version 1.0.1g released on April 7th, 2014. The bug allows any attacker to read the memory of a vulnerable host, which means that any keys that have been used on a host with a vulnerable version of OpenSSL should be considered compromised.

Pivotal Command Center (PCC) requires a PostgreSQL database (postgresql-server) that has a dependency on the OpenSSL library (openssl). Therefore, we are requiring all systems that have PCC installed be checked for the vulnerable OpenSSL require an update to resolve security issues found in the OpenSSL library.

Mitigation

Any system that has Pivotal Command Center installed needs to be immediately checked for the vulnerability reported in **CVE-2014-0160** and if needed a security update should be applied immediately.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name **CVE-2014-0160** to this issue.

The last column in the following table indicates the version to re-mediate the vulnerabilities.

Pivotal Product	Product Version	Running on	Vulnerable Version	Replace with Fixed Version
Pivotal Command Center	2.0.x to 2.1.x	RHEL 6 or CentOS Linux 6 (x86, 64-bit)	`openssl-1.0.1e-15` through `openssl-1.0.1e-16.el6_5.4`	`openssl-1.0.1e-16.el6_5.7`

PCC 2.0.x to 2.1.x is only supported in RHEL 6 or CentOS 6. The vulnerable OpenSSL version was not shipped as part of the 6.4 or older distribution. The first affected distribution is RHEL/CentOS 6.5. However, older 6.x versions could still have been updated to a newer (vulnerable) `openssl-1.0.1` series package.

Note that `openssl-1.0.1e-16.el6_5.7` included a fix backported from `openssl-1.0.1g`.

Solution

1. Determine if your RHEL/CentOS 6.x system is vulnerable to the flaw described in **CVE-2014-0160** using the following command: `rpm -q openssl`
    - If the version is part of the `openssl-1.0.0` series, it is unaffected and you do not need to continue.
    - If the version is `openssl-1.0.1e-16.el6_5.7` (please check the whole version), then it has already been updated with the fix and you are done.
2. **Optional:** Look for and/or query processes which are using the vulnerable libssl library by running either of the following commands as `root`:
    - `lsof | awk 'NR==1 || $0~/libssl.so.1.0.1e/'`
    - `grep libssl.so.1.0.1e /proc/*/maps | cut -d/ -f3 | sort -u | xargs -r -- ps uf`
3. Update the `openssl` package to `openssl-1.0.1e-16.el6_5.7`
    - If you have Internet access:
        - `yum update openssl`
    - Otherwise, download the package directly from a RHEL or CentOS location and transfer the package to the system in question and install it manually:
        - `yum update <path-to-openssl*rpm>`

4. After updating `openssl`, restart all processes using the flawed `libssl.so`:
    - The safest and simplest thing to do is perform a system reboot
    - Alternatively, use the command from step 2 to determine which processes need to be restarted and then act accordingly.
5. **Optional:** Re-scan updated systems with one of the Redhat Heartbleed Detector tools:
    - https://access.redhat.com/labs/heartbleed/
6. Finally, after you have patched and restarted all your servers, you should review your systems for what may have been compromised and take the appropriate steps. For example, you may need to provision new keys and certificates, revoke old server certificates, change any passwords or close any long running sessions. Work with your security team to analyze all security changes required by your systems.

    You may also want to periodically check http://www.kb.cert.org/vuls/id/720951 for up-to-date information on known impact.

References

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- http://www.openssl.org/news/vulnerabilities.html
- http://www.kb.cert.org/vuls/id/720951
- http://heartbleed.com/
- https://access.redhat.com/site/solutions/781793

Contacts

For more information, visit http://www.gopivotal.com/security or contact security at gopivotal.com.