Security: What is the impact of the Heartbeat SSL bug on a Bright cluster?

The Heartbleed bug (CVE-2014-0160) allows anyone to read memory belonging to the server process handling the connection, if they can connect to a server that uses vulnerable versions of the OpenSSL implementation of SSL. On April 11th 2014 software engineers at NCSC-FI demonstrated that private key data can be obtained from a vulnerable server with some effort.

Status of different versions of OpenSSL:

- OpenSSL 1.0.2-beta IS vulnerable
- OpenSSL 1.0.1 through 1.0.1f (inclusive) ARE vulnerable
- OpenSSL 1.0.1g is not vulnerable
- OpenSSL 1.0.0 branch is not vulnerable
- OpenSSL 0.9.8 branch is not vulnerable

(Note that these are versions as used by the upstream OpenSSL project. Distributions may have backported fixes from newer versions into older versions. See below for distribution specific information.)

In Bright Cluster Manager, the CMDaemon server component is one of the components capable of accepting SSL connections. As of Bright Cluster Manager 5.1, CMDaemon makes use of a private OpenSSL implementation (cm-openssl) instead of the OpenSSL implementation that is included with the Linux distribution. For stability reasons, the version of OpenSSL provided by the cm-openssl package in Bright versions up to 6.1 was kept at OpenSSL 1.0.0, which means that CMDaemon itself is not vulnerable to the Heartbleed SSL bug in versions up until (and including) 6.1. The recently released version 7.0 of Bright Cluster Manager initially shipped with a cm-openssl package that included OpenSSL 1.0.1f (which is vulnerable), but a fix has been released which upgrades the OpenSSL package to 1.0.1g (which is not vulnerable).

Most installations of Bright Cluster Manager also run an instance of the Apache web server which provides access to the Bright user portal. By default, the Apache web server has been configured to accept HTTPS connections using the same certificate and private key as is being used by CMDaemon. The SSL implementation that is used by the Apache web server is provided by the OpenSSL package that is part of the Linux base distribution.

Status of base distribution OpenSSL packages:

- RedHat Enterprise Linux 5.* is not vulnerable
- RedHat Enterprise Linux 6.4 and older are not vulnerable
- RedHat Enterprise Linux 6.5 IS vulnerable
- CentOS 5.* is not vulnerable
- CentOS 6.4 and older are not vulnerable

(c) 2019 Bright Computing <kb@brightcomputing.com> | 2019-07-15 22:37
URL: http://kb.brightcomputing.com/faq/index.php?action=artikel&cat=22&id=172&artlang=en

- CentOS 6.5 IS vulnerable
- Scientific Linux 5.* is not vulnerable
- Scientific Linux 6.4 and older are not vulnerable
- Scientific Linux 6.5 IS vulnerable
- SUSE Linux Enterprise Server 11 (all service packs) is not vulnerable

Note that RedHat has already released a fix for this issue. The fix was backported from 1.0.1g and included in openssl-1.0.1e-16.el6_5.7. Derived distributions CentOS and Scientific Linux also inlcuded this revision of the fixed openssl package.

If the Linux base distribution package has not been updated to a revision that includes a fix for Heartbeat SSL bug, the Apache web server that is running on the head node of most Bright clusters is vulnerable to the Heartbeat SSL bug. This means that with sufficient effort, it is possible to obtain the private key data (which is the same private key data that is being used by CMDaemon).

Users of Bright Cluster Manager 7.0 are advised to upgrade to the latest version of the cm-openssl package (1.0.1g), and to upgrade the OpenSSL packages that come as part of the Linux base distribution.

Users of Bright Cluster Manager versions prior to 7.0, that use either RHEL 6.5 or CentOS 6.5 as the Linux base distribution, are advised to upgrade the OpenSSL packages that come as part of the Linux base distribution.

Since it has been demonstrated that private key data can be obtained from an SSL server which is vulnerable to the Heartbleed bug, users of all versions of Bright that have been vulnerable to the Heartbeat SSL bug (e.g. because RHEL 6.5 was being used) are also advised to obtain a new license file (i.e. SSL certificate) and private key information if there is reason to believe that an attacker may have obtained private key information through the Apache web server before the patched OpenSSL package was installed.

Upgrading to the latest version of OpenSSL is normally done as follows:

```
yum update openssl cm-openssl

yum --installroot=/cm/images/default-image update openssl cm-openssl
```

(repeat for each software image other than 'default-image')

(c) 2019 Bright Computing <kb@brightcomputing.com> | 2019-07-15 22:37

URL: http://kb.brightcomputing.com/faq/index.php?action=artikel&cat=22&id=172&artlang=en

Security: What is the impact of the Heartbeat SSL bug on a Bright cluster?

Obtaining a new license file with a new private key can be done as follows:

```
request-license
```

When asked to enter a product key, enter the Bright Cluster Manager product key that was provided to you when you purchased Bright Cluster Manager. When asked whether the private key from the existing license should be re-used, answer No. Note that all client certificates (e.g. admin.pfx for Bright <= 6.0) will be invalidated when a new certificate has been issued with new private key data.

After upgrading OpenSSL packages, all services using it (e.g. Apache) must be restarted. If a new license file with new private key data was installed, all compute nodes must be rebooted in order for them to obtain a new client certificate.

To summarize, users of the following combinations are advised to take appropriate actions because a vulnerability may exist if updates have not yet been applied:

- All Bright 7.0 clusters
- All Bright versions prior to 7.0 with a base distribution of RHEL 6.5, CentOS 6.5 or Scientific Linux 6.5

References:

- General information about the Heartbleed bug: http://heartbleed.com
- RedHat announcement: https://access.redhat.com/site/announcements/781953
- SUSE announcement: http://support.novell.com/security/cve/CVE-2014-0160.html

Unique solution ID: #1171
Author: Martijn de Vries
Last update: 2014-05-28 15:00

(c) 2019 Bright Computing <kb@brightcomputing.com> | 2019-07-15 22:37

URL: http://kb.brightcomputing.com/faq/index.php?action=artikel&cat=22&id=172&artlang=en