Field Notice
Heartbleed Bug Vulnerability in VCS

Background

The OpenSSL Heartbleed bug was fixed by updating the Open Source distribution to suppress the openssl listener-side Transport Layer Security (TLS) support for auxiliary content in heartbeat messages. The intended purpose of this auxiliary data was to facilitate some diagnostic requirements, but the feature exposed the vulnerability described in the following abstracted OpenSSL Security Advisory (from www.openssl.org):

```
OpenSSL Security Advisory 07 Apr 2014

=====================================

TLS heartbeat read overrun (CVE-2014-0160)

=========================================

A missing bounds check in the handling of the TLS heartbeat extension can
be used to reveal up to 64k of memory to a connected client or server.

Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including 1.0.1f
and 1.0.2-beta1.

Thanks for Neel Mehta of Google Security for discovering this bug and to
Adam Langley <agl@chromium.org> and Bodo Moeller <bmoeller@acm.org> for
preparing the fix.

Affected users should upgrade to OpenSSL 1.0.1g. Users unable to
immediately upgrade can alternatively recompile OpenSSL with option:

     -DOPENSSL_NO_HEARTBEATS

1.0.2 will be fixed in 1.0.2-beta2.
```

Only server applications that use the OpenSSL TLS features are vulnerable. The ssh remote shell and other features using the OpenSSL cryptography API are not vulnerable.

VCS Vulnerability

The basic Conductor ISO for all releases beginning with 3.0 includes the 0.9.8 OpenSSL binary (incorporated into the ISO from that version OpenSSL RPM). This version number is displayed you execute an RPM listing on a VCS VM. The 0.9.8 version of OpenSSL does not include the Heartbleed bug vulnerability.

However, the VCS directly embeds a version 1.0.1c OpenSSL binary into the Jabber/XMPP-based message infrastructure packages. These are present on the

Conductor platform ISO image, and are installed only on all VMs as part of configuration for those nodes.

Thus these node types are exposed to the Heartbleed bug vulnerability.

The vulnerability exists for all Conductor releases to date (including version 3.5 RCs).

Recommendation

A patch COP "cisco.conductor-openssl-patch-1.0.1l-3.cop" is available, containing the fix. The patch COP can be applied to any Conductor node, to replace the vulnerable OpenSSL version used by Conductor, with the fixed OpenSSL version 1.0.1l.

Any time a new 3.x system is installed for trial or production purposes, the openssl-patch COP should also be applied, to eliminate exposure to the Heartbleed bug.

Obtaining the Patch

The patch can be obtained from this link https://software.cisco.com/download/navigator.html on cisco.com. The patch COP will also be available in the upcoming Cisco Conductor 3.5 image set.

Installing the Patch

During a maintenance window, execute the following steps. See the README that is delivered with the patch for installation instructions.

Prepare

- Load the patch COP file on to the CMC node.

Apply

- Use the CMC COP administration user interface to install the patch COP onto all Conductor nodes listed on the CMC GUI, on the HOME page. This will require each node to be restarted.

Rollback

- The patch COP may be uninstalled from the CMC user interface. Doing so will remove the OpenSSL 1.0.1l binary, and restore the old binary which had been in use prior to the patch install. This will require all nodes to be restarted.

MsgInfra TLS Certificates

VCS ships with a default certificate file, used by standard Secure Sockets Layer (SSL) Transport Layer Security (TLS) methods for authenticating VCS client Message Infrastructure connections. The default file included with the product should generally have been replaced by one used exclusively for a site, after VCS is installed for trial or production use.

If the OpenSSL Heartbleed vulnerability has been exploited, the possibility exists that secrets may have been collected by an intruder. Replacing the TLS Certificate file will force renegotiation of keys, invalidating the previous certificate. The following section explains how to replace this certificate file, again, with a fresh one exclusive for the site.

Note that if using SASL-based authentication, this file will not be used, as authentication is external to the VCS software. In this case replacing the TLS certificate file serves no purpose.

Replacing the Client TLS Certificate

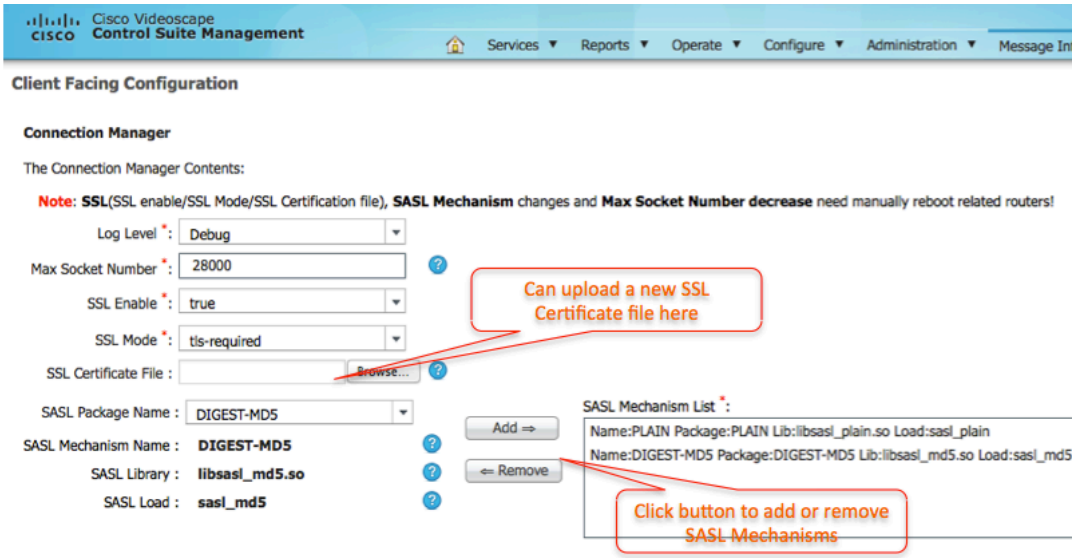
VCS supports replacing the certificate file(s) used by standard Secure Sockets Layer (SSL) Transport Layer Security (TLS) authentication methods for VCS client Message Infrastructure (MsgInfra) connections. VCS ships with a default TLS certificate file, which should generally be replaced by one used exclusively by the site, after VCS is installed for production use.

Log into the CMC. Navigate to the Message Infrastructure "Client Facing Configuration" page by clicking on "Message Infrastructure" on the menu bar:

Select "Client Facing Configuration".

Client Facing Configuration allows one to modify settings related client login, message sending and receiving, affecting the MsgInfra Connection Manager and Session Manager components.

We are interested in the Connection Manager settings shown below:



The above shows a configuration where SSL is enabled, TLS is required, and a SASL package is used for authentication handling. This particular configuration is does not use the TLS Certificate files directly on the MsgInfra server.

However, when SASL is not configured, then a TLS Certificate file will be used, by default the file located in this folder on MsgInfra nodes "/opt/cisco/conductor/xcp/certs/tls".

To apply the new SSL certificate file on the VCS MsgInfra nodes, find the new certificate file by clicking "Browse", and select it. Save the configuration changes and the file will be uploaded to the MsgInfra servers.

You must reboot the MsgInfra VMs in order for the configuration change to take effect on each MsgInfra node. As MsgInfra starts up, it will use the new certificate file, which will be located at the path mentioned above, with the name 'cdert.pem'. This will replace any previous instance of this file, and update the md5 checksum file for the certificate.

> Note: The CMC Message Infrastructure Configuration pages are essentially a front end for the older, MsgInfra Web Controller GUI. If using that GUI (necessary when making certain other configuration changes), old values may be cached in your browser. This requires cleaning the browser cache for MsgInfra Web Controller GUI to re-sync it with what will display in the CMC GUI, after the change.

About This Notice

Audience

This document was written for headend technicians. Field service engineers and Cisco Services engineers may also find the information in this document helpful.

Scope

This document addresses the possible Heartbleed bug vulnerability in the Videoscape Control Suite. This document does not address any possible vulnerabilities in any other Cisco products. For information regarding the Heartbleed bug vulnerability and other Cisco products, visit:

http://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20140409-heartbleed.html

Document Version

This is the second formal release of this document.

For More Information

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

March 2015 Part Number OL-32374-02