Software deferral notice

Dear Cisco Customer,

Cisco engineering has identified a software issue with the release, which you have selected. This issue may affect your use of this software. Please review the deferral notice below to determine if the issue applies to your environment. Customers are urged to upgrade to the recommended solution image or most current software version.

For more comprehensive information about what is included in this software, please refer to the following documents:

- *Cisco TelePresence TC Software Release Notes (TC7)*
- *Cisco TelePresence TC Software Release Notes (TC6)*
- *Cisco TelePresence TC Software Release Notes (TC5)*

Affected software and replacement solution

Reason for Advisory:

The OpenSSL vulnerability commonly known as “heartbleed” affects certain software versions of the TelePresence portfolio.

CDETS No:

CSCuo26378

Headline:

The OpenSSL “heartbleed” issue makes systems running the affected software versions vulnerable to attack

Description:

The listed TelePresence product software versions are affected by the OpenSSL vulnerability CVE-2014-0160, commonly known as the "heartbleed" bug.

This vulnerability can allow attackers to read arbitrary sections of the TelePresence devices memory. Therefore, any sensitive data could be read and this includes SSL private keys, encryption keys, user passwords, certificates etc. This means that both historical data (e.g. stored passwords to access the box) and current communication data (e.g. ongoing H.323 or SIP calls) are vulnerable. Due to the severe nature of this vulnerability, all affected software releases will be removed from cisco.com site.

For more information on the issue, please see:

http://heartbleed.com/

https://www.openssl.org/news/secadv_20140407.txt

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

Disclaimer:

In order to increase availability, Cisco recommends that you upgrade affected images with the suggested replacement software images.

Cisco will discontinue manufacturing shipment of affected images. Any pending order will be substituted by the replacement software images.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred software will apply to the replacement software.

Software type	Software affected	Software solution	
	Version	Version	Availability (dd/mm/yyyy)
TC	5.0.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7 and 5.1.8	5.1.11	29/04/2014
TC	6.0.0, 6.0.1, 6.1.0, 6.1.1, 6.1.2, 6.2.0, 6.2.1 and 6.3.0	6.0.2 (T3), 6.1.3, 6.3.1 (recommended)	TC6.0.2 - 02/06/2014 TC6.1.3 - 02/06/2014 TC6.3.1 - 14/04/2014
TC	7.0.0, 7.0.2 and 7.1.0	7.1.1 and higher	15/04/2014