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)*

Affected software and replacement solution

Reason for Advisory:

The NTP.org and glibc "GHOST" vulnerabilities affects certain software versions.

CDETS No:

CSCus69550 - CVE-2015-0235
CSCus88487 - CVE-2014-9298

Headline:

The NTP.org and glibc "GHOST" vulnerabilities make systems running the affected software versions vulnerable.

Description:

The listed TelePresence product software versions are affected by the NTP.org vulnerability (CVE-2014-9298) and glibc commonly known as the "GHOST" vulnerability (CVE-2015-0235).

January 27, 2015, a buffer overflow vulnerability in the GNU C library (glibc) was publicly announced. This vulnerability is related to the various gethostbyname functions included in glibc and affect applications that call these functions. This vulnerability may allow an attacker to obtain sensitive information from an exploited system or, in some instances, perform remote code execution with the privileges of the application being exploited.

February 4, 2015, an IPv6 ::1 ACL bypass vulnerability was announced. With this vulnerability the IPv6 address ::1 can be spoofed, allowing an attacker to bypass ACLs based on ::1.

For more information on the issue, please see:

CVE-2014-9298:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141222-ntpd

http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities

http://www.insinuator.net/2015/01/should-ipv6-packets-with-source-address-1-be-processed-when-received-on-an-external-interface/

CVE-2015-0235:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150128-ghost

Disclaimer:

In order to increase availability, Cisco recommends that you upgrade affected images with the suggested 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	7.3.0, 7.3.1	7.3.2 and higher	18/03/2015