Software deferral notice

Dear Cisco Customer,

Cisco engineering has identified a software issue with the release that 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

- Cisco TelePresence CE Software Release Notes (CE8)

Affected software and replacement solution

Software type	Software affected	Products affected	Software solution	
	Version		Version	Availability (dd/mm/yyyy)
CE	8.0.0, 8.0.1, 8.1.0	SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800, MX800D	8.1.1	04/05/2016

Reason for Advisory:

A critical security issue has been discovered with the products XML API that may cause an attacker to gain unauthenticated access to the systems configuration and resources.

Headline:

Cisco TelePresence XML API Authentication Bypass Vulnerability - CVE-2016-1387

Description:

Vulnerability in the XML Application Programming Interface (API) of the Cisco TelePresence Codec (TC) and Collaboration Endpoint (CE) System Software could allow an unauthenticated, remote attacker to bypass authentication when accessing the XML API.

For more information on this vulnerability, please refer to the Cisco Security Advisory located at:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-tpxml

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.