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 information about what is included in the resolved software versions, please refer to the

- Cisco TelePresence CE Software Release Notes (CE9)
- Cisco TelePresence CE Software Release Notes (CE8)
- Cisco TelePresence TC Software Release Notes (CE7)

Affected software and replacement solution

Software type	Software affected	Products affected	Software solution	
	Version		Version	Availability (dd/mm/yyyy)
CE9.x	9.1.6, 9.2.5, 9.2.6, 9.3.1, 9.3.2, 9.3.3, 9.4.0, 9.4.1, 9.4.2, 9.5.0, 9.5.1, 9.5.2, 9.5.3, 9.6.1, 9.6.2, 9.6.3, 9.6.4, 9.7.1, 9.7.2, 9.8.0, 9.8.1 9.8.2, 9.9.0, 9.9.1	Cisco Webex Room Series, Cisco Webex Board, Cisco TelePresence SX Series, Cisco TelePresence MX Series, Cisco DX Series	9.8.3 9.9.2 9.10.0	08/01/2020
CE8.x	8.1.1, 8.2.0, 8.2.1, 8.2.2, 8.3.0, 8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7	Cisco TelePresence SX Series, Cisco TelePresence MX Series, Cisco DX Series	8.3.8	08/01/2020
TC7.x	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.3.6, 7.3.7, 7.3.8, 7.3.9 7.3.11, 7.3.12, 7.3.13, 7.3.14, 7.3.15, 7.3.16, 7.3.17, 7.3.18, 7.3.19	Cisco TelePresence SX Series, Cisco TelePresence MX Series, Cisco DX Series, C-Series, EX Series	7.3.20	17/01/2020

Defect references:

CSCvs67675

CSCvs45241

CSCvs67680

Reason for Advisory:

A High impact security issue has been discovered that affects the above software versions. Affected software versions are no longer available to download from https://cisco.com

Headline:

Cisco TelePresence Collaboration Endpoint and TelePresence Codec Path Traversal Vulnerability

CVE ID:

CVE-2020-3143

Security Advisory:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-telepresence-path-tr-wdrnYEZZ

Description:

A vulnerability in the video endpoint API (xAPI) of Cisco TelePresence Collaboration Endpoint (CE) Software, Cisco TelePresence Codec (TC) Software, and Cisco RoomOS Software could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device.

The vulnerability is due to insufficient validation of user-supplied input to the xAPI of the affected software. An attacker could exploit this vulnerability by sending a crafted request to the xAPI. A successful exploit could allow the attacker to read and write arbitrary files in the system. To exploit this vulnerability, an attacker would need either an In-Room Control or administrator account.

Cisco has released software updates that address the vulnerability described in this advisory. There are no workarounds that address this vulnerability.

Please refer to the Security Advisory for more information.

Disclaimer:

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.