Procédure pour activer le soutien du TLS 1.2 des services Web de studio d'appel CVP

Contenu

Introduction

Ce document décrit comment activer le soutien du TLS 1.2 des services Web de studio d'appel du Customer Voice Portal de Cisco (CVP).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Studio d'appel CVP
- Transport Layer Security (TLS)
- Environnement de Runtinme de Javas (JRE)

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Serveur 11.5 CVP
- Studio 11.5 d'appel CVP

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Résumé du problème

Dans l'élément de service Web de studio d'appel, le TLS 1.0 est négocié même si le serveur de service Web prend en charge TLS1.2.

Causes possibles

Utilisations TLS1.0 JRE 7 par défaut.

Action recommandée

Installez le correctif CVP 10.5 – ES24 (désapprouvé) et ES26, CVP 11.0 – ES23, CVP 11.5 – ES7 pour la version 10.5 unifiée CVP, 11.0 et 11.5 respectivement.

Ce correctif force Javas pour placer le contexte pour le TLS 1.2, ainsi toutes les demandes sortantes de https de CVP utiliseront le TLS 1.2.

> **Note**: Ce défaut CSCvc39129was ouvert pour la question.