Dépannage de la vulnérabilité Apache Log4j dans la solution Unified Contact Center Express

Contenu

Introduction

Ce document décrit l'impact de la vulnérabilité Apache Log4j sur la gamme de produits Cisco Contact Center Express (UCCX).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Produit Cisco Unified Contact Center Express version 12.5.X.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Apache a annoncé une vulnérabilité dans le composant Log4j en décembre. Il est largement utilisé dans la solution Cisco Unified Contact Center Express et Cisco participe activement à l'évaluation de la gamme de produits pour vérifier ce qui est sûr et ce qui est affecté.

> **Note**: Plus d'informations sont disponibles sur Cisco Security Advisory - cisco-sa-apache-log4j

Ce document présente plus d'informations au fur et à mesure de sa disponibilité.

Application	ID défaut	11.6.(2)	12.0(1)	12.5(1)	12.5.1(SU1)
UCCX	ID de bogue Cisco CSCwa47388	Non affecté	Non affecté	Aucune correction (reportez-vous à la note)	12.5(1)_SU0 S03
CCP (Social Miner)		Non affecté	Non affecté	Non affecté	12.5(1)_SU0 S03
Gestion De L'Expérience Webex (WxM)		WxM n'utilise pas log4j, donc la solution n'est pas affectée.			

Note: Le correctif pour les clients du train 12.5 ne doit être disponible que sur le 12.5(1)SU1ES03. Les clients sur 12.5(1) doivent passer à 12.5(1)SU1 pour appliquer ES03. Bien que cela nécessite une fenêtre de maintenance, cela ne brise pas la compatibilité avec les autres composants du réseau du client.

Foire aux questions

Q.1 Finesse et CUIC sont-ils également affectés et leur correctif est-il différent pour eux ?

Réponse : Finesse et CUIC sont intégrées dans le bundle logiciel UCCX. Ainsi, le correctif à publier fournira le correctif pour l'ensemble du serveur UCCX.

Q.2 Les versions UCCX inférieures à UCCX 11.6.2 sont-elles également affectées ?

Réponse : Non. Ces versions sont marquées comme non affectées.

Q.3 Quand les correctifs sont-ils publiés ?

Réponse : Le tableau des avis indique les dates provisoires de publication des correctifs. Le tableau doit être mis à jour avec les liens associés.

Q.4 Quelle solution de contournement peut être mise en oeuvre jusqu'à ce que la correction soit prête ?

Réponse : Il est recommandé de suivre l'avis du PSIRT et de s'assurer que les correctifs sont appliqués dès que possible une fois publiés pour les versions concernées.

Q.5 À quelle fréquence le document est-il révisé en fonction des renseignements les plus récents?

Réponse : Le document est examiné quotidiennement et mis à jour le matin (heures IST).

Q.6 La solution CCX est-elle disponible avec les correctifs pour la vulnérabilité CVE-2021-45105, comme log4j a fourni une nouvelle version fixe, c'est-à-dire 2.17.0 ?

Réponse : Oui, le correctif 12.5(1)_SU01_ES03 contient la correction de la vulnérabilité CVE-2021-45105.