Comprendre l'impact de la vulnérabilité Apache Log4j dans la solution Cisco Contact Center

Contenu

Introduction

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

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 version 11.6 et ultérieure.

Informations générales

Apache a récemment annoncé une vulnérabilité dans le composant Log4j. Il est largement utilisé dans la solution de centre de contacts Cisco 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 ici : Cisco Security Advisory - cisco-sa-apache-log4j

Ce document présente plus d'informations au fur et à mesure qu'il devient disponible.

Application	ID défaut	11.6.(2)	12.0(1)	12.5(1)	12.6(1)

UCCE/ICM	CSCwa47273	Correctif - 11.6(2)_ES84 LisezMoi	Correctif - 12.0(1)_ES91 LisezMoi	Correctif - 12.5(1)_ES101 LisezMoi *Remarque 1 : Correctif ES_55 Requis, référez-vous au document de migration OpenJDK* *Remarque 2 : Vérification de la version de Tomcat - Reportez-vous à la section « Vérification de la version de Tomcat sur les serveurs ICM » ci-dessous*	Correctif - 12.6(1)_ES1 LisezMoi
PCCE	CSCwa47274	Correctif - 11.6(2)_ES84 LisezMoi	Correctif - 12.0(1)_ES91 LisezMoi	Correctif - 12.5(1)_ES101 LisezMoi *Remarque 1 : Correctif ES_55 Requis, référez-vous au document de migration OpenJDK* *Remarque 2 : Vérification de la version de Tomcat - Reportez-vous à la section « Vérification de la version de Tomcat sur les serveurs ICM » ci-dessous*	Correctif - 12.6(1)_ES1 LisezMoi
CTIOS		Non affecté	Non affecté	Non affecté	Non affecté
Application	**ID défaut**	**11.6(1)**	**12.0(1)**	**12.5(1)**	**12.6(1)**
CVP	CSCwa47275	Correctif - 11.6(1) ES16 Lisez	Correctif - 12.0(1)_ES10 LisezMoi	Correctif - 12.5(1)_ES25 LisezMoi	Correctif - 12.6(1) LisezMoi
VVB	CSCwa47397	Non affecté	Non affecté	Correctif - 12.5(1)_ES12 Lisez	Correctif - 12.6(1) LisezMoi ** correctif d'utilisation le 29 décem 2021*
Call Studio	CSCwa54008	Callstudio_11.6_Log4j_fix LisezMoi	Callstudio_12.0(1)_Log4j_fix LisezMoi	Callstudio_12.5(1)_Log4j_fix LisezMoi	Callstudio_1)_Log4j_fix LisezMoi
Finesse	CSCwa46459	Non affecté	Non affecté	Non affecté	Correctif - 12.6(1) LisezMoi
CUIC	CSCwa46525	Non affecté	Non affecté	Non affecté	Correctif - 12.6(1) LisezMoi
Données en direct (LD)	CSCwa46810	Correctif - 11.6.1_COP23 LisezMoi	Correctif - 12.0(1)_ES18 LisezMoi	Correctif - 12.5(1)_ES13 LisezMoi	Correctif - 12.6(1) LisezMoi
IDS		Non affecté	Non affecté	Non affecté	Non affecté
Co-res CUIC (CUIC-LD-IDS)	CSCwa46810	Correctif - 11.6.1_COP23 LisezMoi	Correctif - 12.0(1)_ES18 LisezMoi	Correctif - 12.5(1)_ES13 LisezMoi	Correctif - 12.6(1) LisezMoi
CloudConnect	CSCwa51545			Non affecté	Correctif - 12.6(1)_CC
CEE	CSCwa47392	Non affecté	Correctif - 12.0(1)_ES6_ET2	Correctif - 12.5(1)_ES3_ET2	Correctif - 12.6(1)

			LisezMoi	LisezMoi	LisezMoi
CCMP	CSCwa47383	Non affecté	Non affecté	Correctif - 12.5(1)_ES6 LisezMoi	Patch-12.6(1)_ES3 LisezMoi
CCDM	CSCwa47383	Non affecté	Non affecté	Correctif - 12.5(1)_ES6 LisezMoi	Correctif - 12.6(1)_ES3 LisezMoi
Google CCAI	Le jeu de fonctionnalités CCAI confirmé par Google n'est pas affecté				
Gestion De L'Expérience Webex (WxM)	WxM n'ayant pas de log4j utilisateur, la solution n'est pas affectée				
Plateforme de collaboration client (CCP)	CSCwa47384	Non affecté	Non affecté	Non affecté	Non affecté

** Les dates de publication sont sujettes à modification et seront mises à jour au besoin jusqu'à la publication du correctif*

Vérification de la version Tomcat sur les serveurs ICM

1. Sur les serveurs ICM (routeurs, enregistreurs, PG et AW), vérifiez la version de tomcat installée en exécutant le fichier "*<ICM HOME>\tomcat\bin\version.bat*« .
2. Si la version tomcat est **9.0.37 ou supérieure**, procédez comme suit pour corriger le défaut "CSCvv73307"
3. Installez le correctif ES_81 sur le serveur. S'il y a des ES supérieurs à 81 sur le serveur ICM, assurez-vous d'abord de désinstaller ces ES

- 12.5(1)_ES81 Patch - https://software.cisco.com/download/specialrelease/0aab225ecde522734cc6c6491ad1eb42

- 12.5(1)_ES81 ReadMe - https://www.cisco.com/web/software/280840583/158250/Release_Document_1.html

4. Après l'installation réussie de ES_81, confirmez à nouveau la version de tomcat en exécutant le fichier bat *"<ICM HOME>\tomcat\bin\version.bat"*
5. La version de Tomcat doit rester identique à l'étape 1. Si la même version continue avec la réinstallation ordonnée de tous les ES souhaités jusqu'au correctif log4j inclus, à savoir ES_101

Foire aux questions

Q.1 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 américaines)

Q.2 Les versions d'ICM sont-elles les suivantes ? (Routeur, Logger, AW, PG) 10.x, 11.0(x) , 11.5(x) et 11.6(1) affectés ?

Réponse : Ces versions ne sont pas affectées car elles utilisent la version 1.X de log4j.

> **Note**: Le tableau des avis répertorie des bogues spécifiques pour les versions en cours de maintenance. Les versions qui ne sont pas mises en surbrillance sont en fin de maintenance logicielle et ne sont pas prises en compte pour révision.

Q.3 Quand les correctifs sont-ils publiés ?

Réponse : Le tableau des avis indique les dates provisoires de publication des correctifs. Le tableau sera mis à jour avec les liens connexes dès qu'ils seront disponibles.

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 CUIC Autonome 11.6(1) n'est pas affecté par log4j, Cependant le readme de ES indique son correctif requis sur le serveur - pourquoi ?

Réponse : ce ES n'est pas un ES autonome ayant seulement un correctif log4j, ce ES23 est un ES cumulatif comme nous l'aurions pour n'importe quel produit VOS. c'est-à-dire qu'il n'existe qu'un SEE cumulatif et le plus récent disponible pour le Client à tout moment. Considérez ce scénario, dans lequel Cu se trouve dans CUIC autonome 11.6 ES 21 (ou avant) et nécessite les corrections de défauts CUIC de ES22, dans ce cas ils doivent encore installer ES23 (puisque ES sont cumulatifs et que seule la dernière version de ES est disponible pour le client). De plus, ce défaut log4j est mentionné et listé sous LD défectuect dans le fichier ES Readme. Au cours de l'installation ES, les correctifs de défauts sont installés en fonction du déploiement, selon le cas (c'est-à-dire que le déploiement est vérifié si - CUIC autonome /co-res CUIC/LD avant l'installation ES et les correctifs de défauts sont appliqués en conséquence)

Q.6 Quelles mesures dois-je prendre si mon analyseur de sécurité d'entreprise (exemple : Qualys) récupère CVE-2021-45105 après avoir corrigé mon produit UCCE ?

Réponse : Aucune action n'est nécessaire car Cisco a examiné CVE-2021-45105 et a déterminé qu'aucun produit ou offre cloud Cisco n'est affecté par cette vulnérabilité. Cette information a également été mise en évidence dans l'avis. Pour que Log4j version 2.16.0 soit vulnérable à DDoS, une configuration autre que par défaut est requise pour l'exploitabilité. Cela signifie que l'attaquant doit modifier manuellement le fichier de configuration log4j, ce qui n'est pas possible dans les produits UCCE. Par conséquent, CVE-2021-45105 n'est pas applicable.

Q7. Que dois-je faire lorsque je vois des fichiers Log4j « .jar » plus anciens sur mon système, tels que des fichiers 1.2x ?

Réponse : Il est recommandé de conserver les anciens fichiers afin que le processus de restauration ne soit pas interrompu. Une version inactive de ces fichiers sur le système ne rend pas le composant vulnérable.

Cependant, si l'entreprise a besoin de supprimer les fichiers, elle est fortement encouragée à tester le processus souhaité en laboratoire avant de mettre en oeuvre les étapes de production afin de minimiser l'impact. Il est également recommandé de disposer d'un plan de sauvegarde et de restauration pratique pour récupérer le système en cas de problème avec l'activité.