Comprender el impacto de la vulnerabilidad de Apache Log4j en la solución Cisco Contact Center

Contenido

Introducción

Este documento describe el impacto de la vulnerabilidad de Apache Log4j en la línea de productos Cisco Contact Center (UCCE).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Unified Contact Center versión 11.6 y posterior.

Antecedentes

Apache anunció recientemente una vulnerabilidad en el componente Log4j. Se utiliza ampliamente en la solución Cisco Contact Center y Cisco participa activamente en la evaluación de la gama de productos para verificar qué es seguro y qué se ve afectado.

> **Nota:** Puede encontrar más información aquí: Cisco Security Advisory - cisco-sa-apache-log4j

Este documento presenta más información a medida que está disponible .

Aplicación	ID de defecto	11.6.(2)	12.0(1)	12.5(1)	12.6(1)
UCCE/ICM	CSCwa47273	Parche - 11.6(2)_ES84 ReadMe	Parche - 12.0(1)_ES91 ReadMe	Parche - 12.5(1)_ES101 ReadMe *Nota 1: ES_55 patch Required, consulte documento OpenJDK Migration* *Nota 2: Comprobación de la versión de Tomcat: consulte la sección "Comprobación de la versión de Tomcat en servidores ICM" a continuación*	Parche - 12.6(1)_ES1 ReadMe
PCCE	CSCwa47274	Parche - 11.6(2)_ES84 ReadMe	Parche - 12.0(1)_ES91 ReadMe	Parche - 12.5(1)_ES101 ReadMe *Nota 1: ES_55 patch Required, consulte documento OpenJDK Migration* *Nota 2: Comprobación de la versión de Tomcat: consulte la sección "Comprobación de la versión de Tomcat en servidores ICM" a continuación*	Parche - 12.6(1)_ES1 ReadMe
CTIOS		No impactado	No impactado	No impactado	No impactado

Aplicación	ID de defecto	11.6(1)	12.0(1)	12.5(1)	12.6(1)
CVP	CSCwa47275	Parche - 11.6(1) ES16 Léame	Parche - 12.0(1)_ES10 ReadMe	Parche - 12.5(1)_ES25 ReadMe	Parche - 12.6(1)_E ReadMe
VVB	CSCwa47397	No impactado	No impactado	Parche - 12.5(1)_ES12 Léame	Parche - 12.6(1)_E ReadMe ** parche de publicado e de diciembr 2021*
Call Studio	CSCwa54008	Callstudio_11.6_Log4j_fix ReadMe	Callstudio_12.0(1)_Log4j_fix ReadMe	Callstudio_12.5(1)_Log4j_fix ReadMe	Callstudio_1)_Log4j_fix ReadMe
Finesse	CSCwa46459	No impactado	No impactado	No impactado	Parche - 12.6(1)_E ReadMe
CUIC	CSCwa46525	No impactado	No impactado	No impactado	Parche - 12.6(1)_E ReadMe
Datos en directo (LD)	CSCwa46810	Parche - 11.6.1_COP23 ReadMe	Parche - 12.0(1)_ES18 ReadMe	Parche - 12.5(1)_ES13 ReadMe	Parche - 12.6(1)_E ReadMe
IDS		No impactado	No impactado	No impactado	No impactado
Cores CUIC (CUIC-LD-IDS)	CSCwa46810	Parche - 11.6.1_COP23 ReadMe	Parche - 12.0(1)_ES18 ReadMe	Parche - 12.5(1)_ES13 ReadMe	Parche - 12.6(1)_E ReadMe
CloudConnect	CSCwa51545			No impactado	Parche -

					12.6(1)_CC
CEPE	CSCwa47392	No impactado	Parche - 12.0(1)_ES6_ET2 ReadMe	Parche - 12.5(1)_ES3_ET2 ReadMe	Parche - 12.6(1)_E ReadMe
CCMP	CSCwa47383	No impactado	No impactado	Parche - 12.5(1)_ES6 ReadMe	Patch-12.6(1)_ES3 ReadMe
CCDM	CSCwa47383	No impactado	No impactado	Parche - 12.5(1)_ES6 ReadMe	Parche - 12.6(1)_ES3 ReadMe
CCAI de Google	El conjunto de funciones de CCAI confirmado por Google no se ve afectado				
Gestión De Experiencias De Webex (WxM)	WxM no registra al usuario log4j, por lo que la solución no se ve afectada				
Plataforma de colaboración con clientes (CCP)	CSCwa47384	No impactado	No impactado	No impactado	No impactado

** Las fechas de liberación están sujetas a cambios y se actualizarán según sea necesario hasta que se libere el parche*

Comprobación de versiones Tomcat en servidores ICM

1. En los servidores ICM, es decir, los routers, los registradores, los servidores PG y AW, verifican la versión de tomcat instalada ejecutando el archivo "*<ICM HOME>\tomcat\bin\version.bat*".
2. Si la versión de tomcat es **9.0.37 o superior**, realice estos pasos para reparar el defecto "CSCvv73307"
3. Instale el parche ES_81 en el servidor. Si hay algún ES mayor que 81 en el servidor ICM, asegúrese primero de desinstalar esos ES

- 12.5(1)_ES81 Parche - 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. Después de la instalación correcta de ES_81, confirme de nuevo la versión de tomcat ejecutando el archivo bat *"<ICM HOME>\tomcat\bin\version.bat"*
5. La versión de Tomcat debe seguir siendo la misma que la del paso 1. Si lo mismo, continúe con la reinstalación ordenada de todos los ES deseados hasta el parche log4j, incluido el parche de log4j, es decir ES_101

Preguntas frecuentes

P.1 ¿Con qué frecuencia se revisa el documento con la información más reciente?

Respuesta: El documento se revisa diariamente y se actualiza por la mañana (horas de EE. UU.)

P.2 ¿Son las versiones de ICM? (Router, Logger, AW, PG) 10.x, 11.0(x), 11.5(x) y 11.6(1)

afectados?

Respuesta: Estas versiones no se ven afectadas ya que utilizan la versión 1.X de log4j.

> **Nota:** La tabla de asesoría enumera los errores específicos para las versiones que se encuentran bajo mantenimiento. Las versiones que no se resaltan finalizan el mantenimiento del software y no se consideran para su revisión.

P.3 ¿Cuándo se liberan los parches?

Respuesta: La tabla de asesoramiento destaca las fechas provisionales en las que se liberan los parches. La tabla se actualizará con los enlaces correspondientes a medida que estén disponibles.

P.4 ¿Alguna solución alternativa que pueda implementarse hasta que la solución esté lista?

Respuesta: La recomendación es seguir el aviso de PSIRT y asegurarse de que los parches se apliquen tan pronto como sea posible una vez liberados para las versiones afectadas.

Q.5 El CUIC autónomo 11.6(1) no se ve afectado por el log4j. Sin embargo, el readme de ES indica que es un parche obligatorio en el servidor - ¿por qué?

Respuesta: Este ES no es un ES independiente que sólo tiene una corrección de log4j, este ES23 es un ES acumulativo como lo tendríamos para cualquier producto VOS. Es decir, solo hay un ES más reciente y acumulativo disponible para el cliente en cualquier momento. Tenga en cuenta esta situación, en la que Cu se encuentra en el CUIC independiente 11.6 ES 21 (o antes) y requiere las correcciones de defectos CUIC de ES22, en ese caso aún necesitan instalar ES23 (ya que los ES son acumulativos y sólo la última versión de ES está disponible para el cliente). Además, este defecto de log4j se menciona y se enumera bajo defecto LD en el Léame ES. Durante la instalación de ES, las correcciones de defectos se instalan en función de la implementación según corresponda (es decir, se realiza una comprobación de la implementación si - CUIC independiente /co-res CUIC/LD antes de la instalación de ES y se aplican las correcciones de defectos en consecuencia)

P.6 ¿Qué acciones debo llevar a cabo si el escáner de seguridad de mi organización (Ejemplo: Qualys) recoge CVE-2021-45105 después de aplicar parches a mi producto UCCE?

Respuesta: No es necesario realizar ninguna acción, ya que Cisco ha revisado CVE-2021-45105 y ha determinado que esta vulnerabilidad no afecta a productos de Cisco ni a ofertas de nube. Esta información también se ha destacado en el asesoramiento. Para que la versión 2.16.0 de Log4j sea vulnerable a DDoS, se requiere una configuración no predeterminada para aprovechar. Esto significa que el atacante debe modificar manualmente el archivo de configuración de log4j y esto no es posible en los Productos UCCE, por lo que CVE-2021-45105 no es aplicable.

P7. ¿Qué hago cuando veo archivos Log4j ".jar" más antiguos en mi sistema como archivos 1.2x?

Respuesta: La recomendación es dejar los archivos antiguos para que el proceso de reversión no se rompa. El hecho de tener una versión inactiva de estos archivos en el sistema no deja al componente vulnerable.

Sin embargo, si la empresa requiere que se eliminen los archivos, se recomienda encarecidamente probar el proceso deseado en el laboratorio antes de implementar los pasos de

producción para minimizar el impacto. También se recomienda tener un plan de respaldo y reversión a mano para recuperar el sistema en caso de que haya problemas con la actividad.