Solución de problemas de vulnerabilidad de Apache Log4j en la solución Unified Contact Center Express

Contenido

Introducción

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

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 Express versión 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

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

Nota: Hay más información disponible en 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)	12.5.1(SU1)
UCCX	Id. de error de Cisco CSCwa47388	No impactado	No impactado	Sin corrección (consulte la nota)	12.5(1)_SU0 S03
CCP (Social Miner)		No impactado	No impactado	No impactado	12.5(1)_SU0 S03
Gestión De Experiencias De Webex (WxM)		WxM no utiliza log4j, por lo que la solución no se ve afectada.			

Nota: La corrección para los clientes del tren 12.5 estará disponible sólo en 12.5(1)SU1ES03. Los clientes en 12.5(1) deben actualizar a 12.5(1)SU1 para aplicar ES03. Aunque esto requiere una ventana de mantenimiento, no rompe la compatibilidad con ningún otro componente de la red del cliente.

Preguntas frecuentes

P.1 ¿Finesse y CUIC también se ven afectados y son su parche diferente para ellos?

Respuesta: Finesse y CUIC están integrados en el paquete de software UCCX. Por lo tanto, el parche que se lanzará proporcionará la solución para todo el servidor UCCX.

P.2 ¿También se ven afectadas las versiones de UCCX inferiores a las de UCCX 11.6.2?

Respuesta: No. Esas versiones están marcadas como no impactadas.

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 debe actualizarse con los enlaces correspondientes.

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.

P.5 ¿Con qué frecuencia se revisa el documento con la información más reciente?

Respuesta: El documento se revisa diariamente y se actualiza por la mañana (horario de IST).

P.6 ¿Tenemos solución CCX disponible con los parches para la vulnerabilidad CVE-2021-45105, ya que log4j proporcionó nueva versión fija, es decir, 2.17.0 ?

Respuesta: Sí, el parche 12.5(1)_SU01_ES03 consiste en la corrección de la vulnerabilidad de CVE-2021-45105.