Risoluzione dei problemi di vulnerabilità di Apache Log4j nella soluzione Unified Contact Center Express

Sommario

Introduzione

Questo documento descrive l'impatto della vulnerabilità di Apache Log4j sulla linea di prodotti Cisco Contact Center Express (UCCX).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Unified Contact Center Express versione 12.5.X.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Apache ha annunciato una vulnerabilità nel componente Log4j a dicembre. È ampiamente utilizzato nella soluzione Cisco Unified Contact Center Express e Cisco è attivamente impegnato nella valutazione della linea di prodotti per verificare quali sono i componenti sicuri e quali sono i componenti interessati.

Nota: Per ulteriori informazioni, consultare il documento Cisco Security Advisory - cisco-sa-apache-log4j

Ulteriori informazioni sono disponibili nel documento.

Applicazione	ID difetto	11.6.(2)	12.0(1)	12.5(1)	12.5.1(SU1)
UCCX	Cisco, ID bug CSCwa4738	Non interessato	Non interessato	No Fix (nota di riferimento)	12.5(1)_SU0 S03
CCP (Social Miner)		Non interessato	Non interessato	Non interessato	12.5(1)_SU0 S03
Webex Experience Management (WxM)		WxM non utilizza log4j, pertanto la soluzione non ha alcun impatto.			

Nota: La correzione per i clienti del treno 12.5 sarà disponibile solo nella versione 12.5(1)SU1ES03. I clienti della versione 12.5(1) devono eseguire l'aggiornamento alla versione 12.5(1)SU1 per applicare ES03. Anche se ciò richiede un intervallo di manutenzione, non interrompe la compatibilità con altri componenti della rete del cliente.

Domande frequenti

Q.1 Finesse e CUIC sono anch'esse interessate e la loro patch è diversa?

Risposta. Finesse e CUIC sono integrati nel pacchetto software UCCX. Pertanto, la patch da rilasciare fornirà la correzione per l'intero server UCCX.

Q.2 Anche le versioni UCCX inferiori a UCCX 11.6.2 sono interessate?

Risposta. No. Tali versioni sono contrassegnate come senza impatto.

D3. Quando vengono rilasciate le patch?

Risposta. Nella tabella dei consigli sulla sicurezza sono riportate le date provvisorie per il rilascio delle patch. La tabella deve essere aggiornata con i collegamenti correlati.

D4. È possibile implementare soluzioni alternative finché non saranno pronte le patch?

Risposta. Si raccomanda di seguire il consiglio PSIRT e accertarsi che le patch vengano applicate il prima possibile una volta rilasciate per le versioni interessate.

Q.5 Quante volte il documento viene revisionato con le informazioni più recenti?

Risposta. Il documento viene rivisto ogni giorno e aggiornato al mattino (orario IST).

Q.6 Abbiamo la soluzione CCX con le patch per CVE-2021-45105 vulnerabilità come log4j fornito nuova versione fissa, cioè 2.17.0 ?

Risposta. Sì, la patch 12.5(1)_SU01_ES03 consiste nella correzione per la vulnerabilità CVE-2021-45105.