# Comprendere l'impatto della vulnerabilità di Apache Log4j nella soluzione Cisco Contact Center

## Sommario



## Introduzione

In questo documento vengono descritte le conseguenze della vulnerabilità Log4j di Apache sulla linea di prodotti Cisco Contact Center (UCCE).

## 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:

- Prodotto Cisco Unified Contact Center versione 11.6 e successive.

## Premesse

Apache ha recentemente annunciato una vulnerabilità nel componente Log4j. Poiché questo componente è molto usato nella soluzione Cisco Contact Center, Cisco sta attivamente valutando l'intera gamma di prodotti per verificare cosa sia sicuro e cosa sia interessato dalla vulnerabilità.

> **Nota:** per ulteriori informazioni, consultare la pagina Consiglio sulla sicurezza Cisco - cisco-sa-apache-log4j

Il documento sarà aggiornato con altre informazioni non appena si renderanno disponibili.

| Applicazione | ID difetto | 11.6.(2) | 12.0(1) | 12.5(1) | 12.6(1) |
|---|---|---|---|---|---|
| UCCE/ICM | CSCwa47273 | Patch - 11.6(2)_ES84 ReadMe | Patch - 12.0(1)_ES91 ReadMe | Patch - 12.5(1)_ES101 ReadMe<br>*Nota 1: patch ES_55 richiesta, consultare il documento sulla migrazione OpenJDK*<br>*Nota 2: verifica della versione Tomcat; fare riferimento alla sezione "Verifica della versione Tomcat sui server ICM" di seguito* | Patch - 12.6(1)_ES1 ReadMe |
| PCCE | CSCwa47274 | Patch - 11.6(2)_ES84 ReadMe | Patch - 12.0(1)_ES91 ReadMe | Patch - 12.5(1)_ES101 ReadMe<br>*Nota 1: patch ES_55 richiesta, consultare il documento sulla migrazione OpenJDK*<br>*Nota 2: verifica della versione Tomcat; fare riferimento alla sezione "Verifica della versione Tomcat sui server ICM" di seguito* | Patch - 12.6(1)_ES1 ReadMe |
| CTIOS | | Non interessato | Non interessato | Non interessato | Non interessato |

| Applicazione | ID difetto | 11.6(1) | 12.0(1) | 12.5(1) | 12.6(1) |
|---|---|---|---|---|---|
| CVP | CSCwa47275 | Patch - 11.6 (1) ES16 Readme | Patch - 12.0(1)_ES10 ReadMe | Patch - 12.5(1)_ES25 ReadMe | Patch - 12.6(1)_ES ReadMe |
| VVB | CSCwa47397 | Non interessato | Non interessato | Patch - 12.5(1)_ES12 Readme | Patch - 12.6(1)_ES ReadMe<br>**usare la pa pubblicata i dicembre 20* |
| 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 | Non interessato | Non interessato | Non interessato | Patch - 12.6(1)_ES ReadMe |
| CUIC | CSCwa46525 | Non interessato | Non interessato | Non interessato | Patch - 12.6(1)_ES ReadMe |
| Live Data (LD) | CSCwa46810 | Patch - 11.6.1_COP23 ReadMe | Patch - 12.0(1)_ES18 ReadMe | Patch - 12.5(1)_ES13 ReadMe | Patch - 12.6(1)_ES ReadMe |
| IDS | | Non interessato | Non interessato | Non interessato | Non interessato |
| CUIC Co-res (CUIC-LD-IDS) | CSCwa46810 | Patch - 11.6.1_COP23 ReadMe | Patch - 12.0(1)_ES18 ReadMe | Patch - 12.5(1)_ES13 ReadMe | Patch - 12.6(1)_ES ReadMe |
| CloudConnect | CSCwa51545 | | | Non interessato | Patch - 12.6(1)_CC |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | P |
| ECE | CSCwa47392 | Non interessato | Patch - 12.0(1)_ES6_ET2 ReadMe | Patch - 12.5(1)_ES3_ET2 ReadMe | Patch - 12.6(1)_ET ReadMe |
| CCMP | CSCwa47383 | Non interessato | Non interessato | Patch - 12.5(1)_ES6 ReadMe | Patch - 12.6(1)_ES3 ReadMe |
| CCDM | CSCwa47383 | Non interessato | Non interessato | Patch - 12.5(1)_ES6 ReadMe | Patch - 12.6(1)_ES3 ReadMe |
| Google CCAI | Google ha confermato che il set di funzionalità CCAI non è interessato | | | | |
| Webex Experience Management (WxM) | Il protocollo WxM non usa il componente log4j, questa soluzione non è interessata | | | | |
| Customer Collaboration Platform (CCP) | CSCwa47384 | Non interessato | Non interessato | Non interessato | Non interessato |

** Le date di rilascio sono soggette a modifiche e verranno aggiornate in base alle esigenze fino al rilascio della patch*

# Verifica della versione Tomcat sui server ICM

1. Sui server ICM, ad esempio router, logger, server PG e AW, controllare la versione tomcat installata con il file "*<ICM HOME>\tomcat\bin\version.bat*".
2. Se la versione tomcat è **9.0.37 o successive**, attenersi a questa procedura per risolvere il difetto "CSCvv73307".
3. Installare la patch ES_81 sul server. Se sul server ICM sono installate ES superiori a 81, accertarsi di averle prima disinstallate.

- 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. Dopo aver completato l'installazione della patch ES_81, verificare nuovamente la versione tomcat eseguendo il file bat *"<ICM HOME>\tomcat\bin\version.bat".*
5. La versione Tomcat deve rimanere invariata rispetto al passaggio 1. Se la versione è la stessa, continuare a reinstallare ordinatamente tutte le patch ES desiderate fino a installare la patch log4j, ossia la ES_101.

# Domande frequenti

D1. Con quale frequenza viene aggiornato questo documento con le ultime informazioni?

Risposta. Il documento viene rivisto quotidianamente e aggiornato la mattina (fuso orario USA).

D2. Le versioni ICM (Router, Logger, AW, PG) 10.x , 11.0(x) , 11.5(x) e 11.6(1) interessate?

Risposta. Queste versioni non sono interessate perché usano la versione 1.X di log4j.

> **Nota:** nella tabella dei consigli sulla sicurezza sono specificati i bug delle versioni ancora in corso di aggiornamento. Le versioni non evidenziate non rientrano più nei programmi di manutenzione e non vengono prese in considerazione.

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 verrà aggiornata con i relativi collegamenti non appena questi saranno disponibili.

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.

D5. CUIC Standalone 11.6(1) non usa il componente log4j. Tuttavia, nel file readme dell'ES è scritto che è richiesta una patch sul server, perché?

Risposta. Questa ES non è una ES standalone che contiene solo la correzione per log4j, ES23 è una patch cumulativa come per qualsiasi altro prodotto VOS. Dal punto di vista del cliente, in qualsiasi momento sarà disponibile solo l'ES più recente e cumulativa. Supponiamo di avere un CUIC Standalone 11.6 ES 21 (o precedenti) che richiedano la correzione ES22 dei difetti CUIC; in questo caso, sarà necessario installare comunque ES23 (in quanto le patch ES sono cumulative e solo l'ultima versione è disponibile per il cliente). Inoltre, questo difetto log4j è citato ed elencato nel difetto LD del file Readme di ES. Durante l'installazione di ES, le correzioni dei difetti vengono installate in base alla distribuzione applicabile (ad esempio, viene eseguito un controllo della distribuzione se - CUIC standalone /co-res CUIC/LD prima dell'installazione di ES e le correzioni dei difetti vengono applicate di conseguenza)

D6. Cosa fare se lo scanner di sicurezza dell'azienda, ad esempio Qualys, rileva un difetto CVE-2021-45105 dopo aver installato le patch sul prodotto UCCE?

Risposta. Non è necessaria alcuna azione in quanto Cisco ha analizzato il bug CVE-2021-45105 e ha stabilito che questa vulnerabilità non influisce sui prodotti o le offerte cloud di Cisco. Queste informazioni sono state evidenziate anche nel consiglio sulla sicurezza. Affinché Log4j versione 2.16.0 sia vulnerabile agli attacchi DDoS, è necessaria una configurazione non predefinita per l'exploit. Ciò significa che l'hacker deve modificare manualmente il file di configurazione log4j e ciò non è possibile nei prodotti UCCE, pertanto la vulnerabilità CVE-2021-45105 non influisce minimamente.

D7. Cosa fare quando si notano file ".jar" di Log4j più vecchi sul sistema, ad esempio file 1.2x?

Risposta. Si consiglia di lasciare i vecchi file in modo che il processo di rollback non venga interrotto. Mantenere una versione inattiva di questi file sul sistema non rende vulnerabile il componente.

Tuttavia, se l'azienda richiede la rimozione dei file, si consiglia vivamente di provare il processo in laboratorio prima di implementarlo in produzione per ridurre al minimo eventuali effetti negativi. Si consiglia inoltre di avere piani di backup e rollback per ripristinare il sistema in caso l'attività generasse errori o problemi.