

瞭解Cisco Contact Center解決方案中Apache Log4j漏洞的影響

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[ICM 伺服器的 Tomcat 版本檢查](#)

[常見問題](#)

簡介

本文件說明 Apache Log4j 漏洞對思科客服中心 (UCCE) 產品線的影響。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Unified Contact Center 產品版本 11.6 及更新版本。

背景資訊

Apache 最近公告了 Log4j 元件中的漏洞。此元件廣泛用於思科客服中心解決方案，而思科也正在積極評估系列產品，以確認安全的項目與受影響的項目。

附註：有關詳細資訊，請參閱：[思科安全建議 — cisco-sa-apache-log4j](#)

本文件會在有可用內容時提供更多資訊。

	ID	11.6.(2)	12.0(1)	12.5(1)	12.6(1)
UCCE/ICM	CSCwa47273	修補程式 - 11.6(2) ES84 讀我檔案	修補程式 - 12.0(1) ES91 讀我檔案	修補程式 - 12.5(1) ES101 讀我檔案 附註1:需要ES_55修補程式，請參閱 OpenJDK遷移文檔 附註2: Tomcat 版本檢查 - 請	修補程式 - 12.6(1) ES 讀我檔案

參閱以下的「JCM 伺服器上的 Tomcat 版本檢查」一節

PCCE	CSCwa47274	修補程式 - 11.6(2) ES84 讀我檔案	修補程式 - 12.0(1) ES91 讀我檔案	修補程式 - 12.5(1) ES101 讀我檔案 附註1:需要ES_55修補程式, 請參閱 OpenJDK遷移文檔 附註2: Tomcat 版本檢查 - 請參閱以下的「JCM 伺服器上的 Tomcat 版本檢查」一節	修補程式 - 12.6(1) ES102 讀我檔案
CTIOS		未受影響	未受影響	未受影響	未受影響
	ID	11.6(1)	12.0(1)	12.5(1)	12.6(1)
CVP	CSCwa47275	修補程式 - 11.6(1) ES16 讀我檔案	修補程式 - 12.0(1) ES10 讀我檔案	修補程式 - 12.5(1) ES25 讀我檔案	修補程式 - 12.6(1) ES26 讀我檔案
VVB	CSCwa47397	未受影響	未受影響	修補程式 - 12.5(1) ES12 讀我檔案	修補程式 - 12.6(1) ES13 讀我檔案 * 使用於 2012 年 12 月 29 日的修補程式
Call Studio	CSCwa54008	Callstudio 11.6 L og4j fix 讀我檔案	Callstudio 12.0(1) Log4j fix 讀我檔案	Callstudio 12.5(1) Log4j fix 讀我檔案	Callstudio 12.6(1) Log4j fix 讀我檔案
Finesse	CSCwa46459	未受影響	未受影響	未受影響	修補程式 - 12.6(1) ES14 讀我檔案
CUIC	CSCwa46525	未受影響	未受影響	未受影響	修補程式 - 12.6(1) ES15 讀我檔案
即時資料 (LD)	CSCwa46810	修補程式 - 11.6.1 COP23 讀我檔案	修補程式 - 12.0(1) ES18 讀我檔案	修補程式 - 12.5(1) ES13 讀我檔案	修補程式 - 12.6(1) ES14 讀我檔案
IDS		未受影響	未受影響	未受影響	未受影響
CUIC Co-res (CUIC-LD-IDS)	CSCwa46810	修補程式 - 11.6.1 COP23 讀我檔案	修補程式 - 12.0(1) ES18 讀我檔案	修補程式 - 12.5(1) ES13 讀我檔案	修補程式 - 12.6(1) ES14 讀我檔案
CloudConnect	CSCwa51545			未受影響	修補程式 - 12.6(1) CC15 讀我檔案
ECE	CSCwa47392	未受影響	修補程式 - 12.0(1) ES6 ET2 讀我檔案	修補程式 - 12.5(1) ES3 ET2 讀我檔案	修補程式 - 12.6(1) ES4 讀我檔案

CCMP	CSCwa47383	未受影響	未受影響	修補程式 - 12.5(1) ES6 讀我檔案	修補程式 - 12.6(1) ES6 讀我檔案
CCDM	CSCwa47383	未受影響	未受影響	修補程式 - 12.5(1) ES6 讀我檔案	修補程式 - 12.6(1) ES6 讀我檔案
Google CCAI	Google 已確認 CCAI 功能集未受影響				
Webex Experience Management (WxM)	WxM 並非使用者 log4j，因此解決方案未受影響				
Customer Collaboration Platform (CCP)	CSCwa47384	未受影響	未受影響	未受影響	未受影響

* 發佈日期可能會有所異動，並且將視需要更新，直到發佈修補程式為止

ICM 伺服器的 Tomcat 版本檢查

1. 在 ICM 伺服器 (即路由器、記錄器、PG 及 AW 伺服器) 上，執行 「<ICM HOME>\tomcat\bin\version.bat」 檔案以檢查安裝的 Tomcat 版本。
2. 如果 Tomcat 版本為 **9.0.37 或更新版本**，請執行下列步驟以修正瑕疵 「[CSCvv73307](#)」
3. 將 ES_81 修補程式安裝在伺服器上。如果 ICM 上有任何大於 81 的 ES，請務必先解除安裝這些 ES。

- 12.5(1)_ES81 修補程式 -

<https://software.cisco.com/download/specialrelease/0aab225ecde522734cc6c6491ad1eb42>

- 12.5(1)_ES81 讀我檔案 -

https://www.cisco.com/web/software/280840583/158250/Release_Document_1.html

4. 成功安裝 ES_81 後，請執行 BAT 檔案 「<ICM HOME>\tomcat\bin\version.bat」 以再次確認 Tomcat 版本
5. Tomcat 版本應與步驟 1 保持一致；如果相同，請繼續循序重新安裝所有需要的 ES，最高包括 log4j 修補程式 (即 ES_101)

常見問題

問。1 多長時間修訂一次載有最新資訊的檔案？

答案： 我們每日都會檢閱文件並在上午 (美國時間) 進行更新

問題 2： ICM (即路由器、記錄器、AW、PG) (路由器、記錄器、AW、PG) 10.x、11.0(x)、11.5(x)和11.6(1)受影響？

答案： 這些版本不會受到影響，因為其使用 1.X 版的 log4j。

附註： 公告表格會列出維護中版本的特定錯誤。未強調顯示之版本的軟體維護已結束，將不會列入檢閱考量。

問題 3：何時會發佈修補程式？

答案：公告表格會強調顯示發佈修補程式的暫訂日期。此表格會在有相關連結可用時進行更新。

問題 4：在修正準備就緒之前，是否可以實作任何因應措施？

答案：建議遵循 PSIRT 公告指示，並確保在受影響版本的修補程式發佈後盡快加以套用。

Q.5 CUIIC Standalone 11.6(1)不受log4j的影響，但[ES的自述檔案](#)說明了在伺服器上需要補丁程式—原因？

答案：此 ES 並非僅包含 log4j 修正的獨立 ES，此 ES23 為累加式 ES，與我們用於任何 VOS 產品的項目一樣。也就是說，客戶任何時候都只有一個最新的累加式 ES 可使用。請思考一下此情境：客戶在獨立 CUIIC 11.6 ES 21（或之前的版本）中，並且需要 ES22 的 CUIIC 瑕疵修正，在該情況下，他們仍需要安裝 ES23（因為 ES 為累加式，而且客戶只能使用最新版本的 ES）。另外，在 ES 讀我檔案中的 LD 瑕疵下會提及並列出此 log4j 瑕疵。在 ES 安裝期間，根據適用的部署安裝缺陷修復（即進行部署檢查，以確定 — 安裝 ES 之前是否使用獨立 CUIIC /co-res CUIIC/LD，並相應地應用缺陷修復）

問題 6：在修補 UCCE 產品後，如果我的組織安全性掃描程式（例如：Qualys）選取 CVE-2021-45105，我要採取哪些動作？

答案：您不必採取任何動作，因為思科已檢閱 CVE-2021-45105 並判定此漏洞不會影響任何思科產品或雲端產品及服務。我們也已在公告中強調顯示此資訊。由於 Log4j 版本 2.16.0 易受到 DDoS 攻擊，因此必須使用非預設組態才能抵禦惡意攻擊。這意味著，攻擊者必須手動修改 log4j 組態檔案，但在 UCCE 產品中無法執行此動作，因此 CVE-2021-45105 並不適用。

問題 7：如果我在系統上看到較舊的 Log4j「.jar」檔案（例如 1.2x 檔案），我該怎麼做？

答案：建議保留舊檔案，以避免復原程序中斷。系統上有這些檔案的非作用中版本並不會讓元件易受攻擊。

但是，如果業務上需要移除這些檔案，則在生產環境中實作步驟之前，強烈建議先在實驗室中測試所需程序，以將影響降至最低。此外，建議您準備好備份和復原計畫，以便在活動發生問題時復原系統。