Analyse der Schwachstellen von Apache Log4j in der Cisco Contact Center-Lösung

Inhalt

Einleitung

In diesem Dokument werden die Auswirkungen der Schwachstelle von Apache Log4j auf die Cisco Contact Center (UCCE)-Produktlinie beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Unified Contact Center-Produktversion 11.6 und höher

Hintergrundinformationen

Apache hat vor kurzem eine Schwachstelle in Log4j angekündigt. Sie wird häufig in der Cisco Contact Center-Lösung verwendet, und Cisco bewertet das Produktportfolio aktiv, um die Sicherheit und die Auswirkungen zu überprüfen.

> **Anmerkung:** Weitere Informationen finden Sie hier: Cisco Security Advisory - cisco-sa-apache-log4j

Dieses Dokument enthält weitere Informationen, sobald es verfügbar ist.

Anwendung	Defekt-ID	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 *Anmerkung 1: ES_55-Patch erforderlich, siehe OpenJDK Migration doc* *Anmerkung 2: Tomcat Versionsprüfung - Siehe Abschnitt "Tomcat Version Check on ICM Servers" unten*	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 *Anmerkung 1: ES_55-Patch erforderlich, siehe OpenJDK Migration doc* *Anmerkung 2: Tomcat Versionsprüfung - Siehe Abschnitt "Tomcat Version Check on ICM Servers" unten*	Patch - 12.6(1)_ES1 ReadMe
CTIS		Nicht betroffen	Nicht betroffen	Nicht betroffen	Nicht betroffen

Anwendung	**Defekt-ID**	**11.6(1)**	**12.0(1)**	**12.5(1)**	**12.6(1)**
CVP	CSCwa47275	Patch - 11.6(1) ES16 Lesen	Patch - 12.0(1)_ES10 ReadMe	Patch - 12.5(1)_ES25 ReadMe	Patch - 12.6(1)_ES ReadMe
VVB	CSCwa47397	Nicht betroffen	Nicht betroffen	Patch - 12.5(1)_ES12 Lesen	Patch - 12.6(1)_ES ReadMe ** Verwendu des Patches 29. Dez. 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	Nicht betroffen	Nicht betroffen	Nicht betroffen	Patch - 12.6(1)_ES ReadMe
CUIC	CSCwa46525	Nicht betroffen	Nicht betroffen	Nicht betroffen	Patch - 12.6(1)_ES ReadMe
Live-Daten (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		Nicht betroffen	Nicht betroffen	Nicht betroffen	Nicht betroffen
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			Nicht betroffen	Patch - 12.6(1)_CC
ECE	CSCwa47392	Nicht betroffen	Patch - 12.0(1)_ES6_ET2 ReadMe	Patch - 12.5(1)_ES3_ET2 ReadMe	Patch - 12.6(1)_ET ReadMe

CCMP	CSCwa47383	Nicht betroffen	Nicht betroffen	Patch - 12.5(1)_ES6 ReadMe	Patch-12.6(1)_ES3 ReadMe
CCDM	CSCwa47383	Nicht betroffen	Nicht betroffen	Patch - 12.5(1)_ES6 ReadMe	Patch - 12.6(1)_ES3 ReadMe
Google CCAI	Das von Google bestätigte CCAI-Feature-Set ist nicht betroffen.				
WebEx Experience Management (WXM)	WxM verwendet log4j nicht, daher ist die Lösung nicht betroffen.				
Customer Collaboration-Plattform (CCP)	CSCwa47384	Nicht betroffen	Nicht betroffen	Nicht betroffen	Nicht betroffen

** Veröffentlichungsdaten können sich ändern und werden bei Bedarf aktualisiert, bis der Patch veröffentlicht wird.*

Tomcat-Versionsprüfung auf ICM-Servern

1. Auf ICM-Servern, d. h. Routern, Loggers, PG- und AW-Servern, überprüfen Sie die installierte Version von Tomcat, indem Sie die Datei *"ICM HOME>\tomcat\bin\version.bat*" ausführen.
2. Wenn die Tomcat-Version **9.0.37 oder höher** ist, führen Sie die folgenden Schritte aus, um den Fehler "CSCvv7307" zu beheben.
3. Installieren Sie den Patch ES_81 auf dem Server. Wenn ESs größer als 81 auf dem ICM-Server vorhanden sind, stellen Sie sicher, dass diese ESs zuerst deinstalliert werden

- 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. Nach der erfolgreichen Installation von ES_81 bestätigen Sie die Tomcat-Version erneut, indem Sie die BAT-Datei ausführen *"<ICM HOME>\tomcat\bin\version.bat"*
5. Die Tomcat-Version sollte mit Schritt 1 identisch sein. Wenn Sie mit der ordnungsgemäßen Neuinstallation aller gewünschten ESs bis einschließlich log4j-Patch, d. h. ES_101, fortfahren

Häufige Fragen

F.1 Wie oft wird das Dokument mit den neuesten Informationen überarbeitet?

Antwort: Das Dokument wird täglich geprüft und morgens (in den USA) aktualisiert.

Q.2 sind die ICM-Versionen, d.h. (Router, Logger, AW, PG) 10.x, 11.0(x), 11.5(x) und 11.6(1) betroffen?

Antwort: Diese Versionen sind nicht betroffen, da sie die 1.x-Version von log4j verwenden.

Anmerkung: Die Tabelle mit Sicherheitsratschlägen listet spezifische Fehler für die zu wartenden Versionen auf. Nicht hervorgehobene Versionen sind das Ende der Softwarewartung und werden nicht zur Prüfung herangezogen.

Q.3 Wann werden Patches veröffentlicht?

Antwort: Der Beratungstabelle zeigt ein zaghaftes Datum für die Veröffentlichung der Patches. Die Tabelle wird mit den entsprechenden Links aktualisiert, sobald diese verfügbar sind.

Q.4 Welche Problemumgehung kann implementiert werden, bis die Behebung fertig ist?

Antwort: Es wird empfohlen, dem PSIRT-Ratgeber zu folgen und sicherzustellen, dass Patches so schnell wie möglich angewendet werden, sobald sie für betroffene Versionen veröffentlicht wurden.

Q.5 CUIC Standalone 11.6(1) ist von log4j nicht betroffen, aber die Readme von ES gibt seinen erforderlichen Patch auf dem Server an - warum?

Antwort: Dieses ES ist kein eigenständiges ES, das nur log4j behebt, dieses ES23 ist ein kumulatives ES, wie wir es für jedes VOS-Produkt hätten. d. h. dem Kunden steht zu jedem Zeitpunkt nur eine letzte und kumulative ES zur Verfügung. Betrachten Sie dieses Szenario, in dem Cu im eigenständigen CUIC 11.6 ES 21 (oder früher) ist und die CUIC-Fehlerbehebungen des ES22 erfordert, in diesem Fall müssen sie weiterhin ES23 installieren (da ES kumulativ ist und nur die neueste Version von ES für den Kunden verfügbar ist). Darüber hinaus wird dieser log4j-Defekt erwähnt und unter LD-Defekt im ES Readme aufgeführt. Während der ES-Installation werden Fehlerbehebungen je nach Anwendung der Bereitstellung installiert (d. h. die Bereitstellungsüberprüfung wird durchgeführt, ob - Standalone CUIC/co-res CUIC/LD vor der ES-Installation angewendet und entsprechende Fehlerbehebungen angewendet werden).

F.6 Welche Maßnahmen ergreife ich, wenn der Sicherheitsscanner meiner Organisation verwendet wird (Beispiel: Qualys) erhält CVE-2021-45105, nachdem ich mein UCCE-Produkt gepatcht habe?

Antwort: Cisco hat die CVE-2021-45105 geprüft und festgestellt, dass diese Schwachstelle keine Cisco Produkte oder Cloud-Angebote beeinträchtigt. Diese Informationen wurden auch im Ratgeber hervorgehoben. Damit Log4j Version 2.16.0 für DDoS anfällig ist, ist eine nicht standardmäßige Konfiguration erforderlich, um Exploitability zu erreichen. Dies bedeutet, dass der Angreifer die log4j-Konfigurationsdatei manuell ändern sollte, was in UCCE-Produkten nicht möglich ist. Daher ist CVE-2021-45105 nicht anwendbar.

Frage 7. Was kann ich tun, wenn ich ältere Log4j ".jar"-Dateien auf meinem System sehe, z. B. 1.2x-Dateien?

Antwort: Es wird empfohlen, die alten Dateien zu belassen, damit der Rollback-Prozess nicht unterbrochen wird. Eine inaktive Version dieser Dateien auf dem System lässt die Komponente nicht verwundbar.

Wenn Unternehmen jedoch die Entfernung der Dateien erfordern, wird dringend empfohlen, den gewünschten Prozess im Labor zu testen, bevor die einzelnen Schritte in der Produktionsumgebung implementiert werden, um die Auswirkungen zu minimieren. Es wird außerdem empfohlen, einen Backup- und Rollback-Plan griffbereit zu haben, um das System wiederherzustellen, falls Probleme mit der Aktivität auftreten.