Understand the Impact of Apache Log4j Vulnerability in Cisco Contact Center Solution

Contents

Introduction

This document describes the impact of Apache Log4j vulnerability on Cisco Contact Center (UCCE) product line.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Contact Center product version 11.6 and higher.

Background Information

Apache recently announced a vulnerability in Log4j component. It is widely used in Cisco Contact Center solution and Cisco is actively in the evaluation of the product lineup to verify what is safe and what is affected.

> **Note**: More information is available here: Cisco Security Advisory - cisco-sa-apache-log4j

This document presents more information as it becomes available .

Application	Defect 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 *Note 1: ES_55 patch Required, refer OpenJDK Migration doc* *Note 2: Tomcat Version Check- Refer section "Tomcat Version Check on ICM Servers" below*	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 *Note 1: ES_55 patch Required, refer OpenJDK Migration doc* *Note 2: Tomcat Version Check- Refer section "Tomcat Version Check on ICM Servers" below*	Patch - 12.6(1)_ES1 ReadMe
CTIOS		Not impacted	Not impacted	Not impacted	Not impacted

Application	**Defect Id**	**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	Not impacted	Not impacted	Patch - 12.5(1)_ES12 Readme	Patch - 12.6(1)_ES ReadMe * use patch published o Dec 2021
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	Not impacted	Not impacted	Not impacted	Patch - 12.6(1)_ES ReadMe
CUIC	CSCwa46525	Not impacted	Not impacted	Not impacted	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		Not impacted	Not impacted	Not impacted	Not impacted
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			Not impacted	Patch - _12.6(1)_CC P
ECE	CSCwa47392	Not impacted	Patch - 12.0(1)_ES6_ET2	Patch - 12.5(1)_ES3_ET2	Patch - 12.6(1)_ET

			ReadMe	ReadMe	ReadMe
CCMP	CSCwa47383	Not impacted	Not impacted	Patch - 12.5(1)_ES6 ReadMe	Patch-12.6(1)_ES3 ReadMe
CCDM	CSCwa47383	Not impacted	Not impacted	Patch - 12.5(1)_ES6 ReadMe	Patch - 12.6(1)_ES3 ReadMe
Google CCAI	Google confirmed CCAI feature set is Not impacted				
Webex Experience Management (WxM)	WxM does not user log4j hence solution is Not impacted				
Customer Collaboration Platform (CCP)	CSCwa47384	Not impacted	Not impacted	Not impacted	Not impacted

** Dates of release are subject to change and will be updated as needed until patch is released*

Tomcat Version Check on ICM Servers

1. On ICM servers i.e. Routers, Loggers, PG and AW servers check the version of tomcat installed by running "*<ICM HOME>\tomcat\bin\version.bat*" file.
2. If the tomcat version is **9.0.37 or higher**, perform these steps to fix the defect "CSCvv73307"
3. Install ES_81 patch on the server. If there are any ES's greater than 81 on the ICM server do ensure first to uninstall those ES's

- 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. After successful install of ES_81 confirm the tomcat version again by running the bat file *"<ICM HOME>\tomcat\bin\version.bat"*
5. Tomcat version should remain the same as step 1, If same proceed with orderly reinstall of all the desired ES's upto and including log4j patch i.e. ES_101

Frequent Asked Questions

Q.1 How often is the document revised with latest information?

Answer: The document is reviewed daily and updated in the morning (US hours)

Q.2 Are the ICM versions i.e. (Router ,Logger, AW, PG) 10.x , 11.0(x) , 11.5(x) and 11.6(1) affected?

Answer: These versions are not impacted as they use 1.X version of log4j.

Note: The advisory table lists specific bugs for the versions which are under maintenance. Versions which are not highlighted are end of software maintenance and are not considered for review.

Q.3 When are patches released?

Answer: The advisory table highlights tentative dates when the patches are released. The table will be updated with the related links as they become available.

Q.4 Any workaround which can be implemented until the fix is ready ?

Answer: Recommendation is to follow the PSIRT advisory and ensure that patches are applied as soon as possible once released for affected versions.

Q.5 CUIC Standalone 11.6(1) is not affected y log4j, However the readme of ES states its a required patch on the server - why ?

Answer: This ES is not a standalone ES having only log4j fix, this ES23 is a cumulative ES like we would have for any VOS product. i.e There is only one latest and cumulative ES available to the Customer at any point of time. Consider this scenario, wherein Cu is in Standalone CUIC 11.6 ES 21 (or before) and are requiring the CUIC defect fixes of ES22, in that case they still need to install ES23 (as ES are cumulative and only latest version of ES are available for the customer) . Moreover this log4j defect is mentioned and listed under LD defect in the ES Readme. During ES installation, defect fixes are installed based on the deployment as applicable (i.e deployment check is made whether - Standalone CUIC /co-res CUIC/LD prior to ES installation and defect fixes are applied accordingly)

Q.6 What actions do I take if my organizations security scanner (Example: Qualys) picks up CVE-2021-45105 after I patched my UCCE Product?

Answer: No action is needed as Cisco has reviewed CVE-2021-45105 and has determined that no Cisco products or cloud offerings are impacted by this vulnerability. This information has been highlighted in the advisory as well. For Log4j version 2.16.0 to be DDoS vulnerable a non-default configuration is required for exploitability. This means that the attacker should manually modify the log4j configuration file and this is not possible in UCCE Products, hence CVE-2021-45105 is not applicable.

Q7. What do I do when I see older Log4j ".jar" files on my system such as 1.2x files?

Answer: Recommendation is to leave the old files so that the rollback process would not be broken. Having an inactive version of these files on the system does not leave the component vulnerable.

However, if business requires the files need to be removed it strongly encouraged to test the desired process in lab prior to implement the steps in production to minimize impact. It is also recommended to have backup and rollback plan handy to recover the system in case there are issues with the activity.