Troubleshoot Apache Log4j Vulnerability in Unified Contact Center Express Solution

Contents

Introduction

This document describes the impact of Apache Log4j vulnerability on Cisco Contact Center Express (UCCX) 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 Express product version 12.5.X.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Apache announced a vulnerability in Log4j component in December. It is widely used in Cisco Unified Contact Center Express 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 on Cisco Security Advisory - cisco-sa-apache-log4j

This document presents more information as it becomes availabe .

Application	**Defect Id**	**11.6.(2)**	**12.0(1)**	**12.5(1)**	**12.5.1(SU1)**

UCCX	Cisco Bug ID CSCwa47388	Not Impacted	Not Impacted	No Fix (refer Note)	12.5(1)_SU S03
CCP (Social Miner)		Not Impacted	Not Impacted	Not Impacted	12.5(1)_SU S03
Webex Experience Management (WxM)		WxM does not use log4j hence solution is Not Impacted.			

Note: The fix for customers on the 12.5 train shall be available only on 12.5(1)SU1ES03. Customers on 12.5(1) must upgrade to 12.5(1)SU1 in order to apply ES03. While this does requires a maintenance window it does not break compatibility to any other components in the customer network.

Frequent Asked Questions

Q.1 Are Finesse and CUIC also affected and is their different patch for them ?

Answer: Finesse and CUIC are integrated in the UCCX software bundle. Thus the patch to be released will provide the fix for entire UCCX Server.

Q.2 Are the UCCX Versions lower than UCCX 11.6.2 also impacted?

Answer: No. Those versions are marked not-impacted.

Q.3 When are patches released?

Answer: The advisory table highlights tentative dates when the patches are released. The table should be updated with the related links.

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 How often is the document revised with latest information?

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

Q.6 Do we have CCX solution come out with the patches for CVE-2021-45105 vulnerability as log4j provided new fixed version i.e. 2.17.0 ?

Answer: Yes the12.5(1)_SU01_ES03 patch consists the fix for CVE-2021-45105 vulnerability.