Cisco Contact Center 솔루션에서 Apache Log4j 취약성의 영향 이해

목차

소개

이 문서에서는 Apache Log4j 취약성이 Cisco UCCE(Contact Center) 제품 라인에 미치는 영향에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Unified Contact Center 제품 버전 11.6 이상

배경 정보

Apache는 최근 Log4j 구성 요소에 취약성을 발표했습니다. Cisco Contact Center 솔루션에서 널리 사용되고 있으며, Cisco는 무엇이 안전하고 어떤 영향을 받는지 확인하기 위해 제품 라인업을 평가하는 데 적극 참여하고 있습니다.

> **참고:** 자세한 내용은 Cisco Security Advisory - cisco-sa-apache-log4j를 참조하십시오.

이 문서는 사용 가능한 추가 정보를 제공합니다.

	ID	11.6.(2)	12.0(1)	12.5(1)	12.6(1)
UCCE/ICM	CSCwa47273	패치 -	패치 - 12.0(1) ES91 읽어보기	패치 - 12.5(1) ES101 읽어보기	패치 -

		11.6(2)_ES84 읽어보기		*참고 1: ES_55 패치 필요, OpenJDK 마이그레이션 문서 참조* *참고 2: Tomcat 버전 확인- 아래의 "ICM 서버에서 Tomcat 버전 확인" 섹션을 참조하십시오.*	12.6(1)_ES1 읽어보기
PCCE	CSCwa47274	패치 - 11.6(2)_ES84 읽어보기	패치 - 12.0(1)_ES91 읽어보기	패치 - 12.5(1)_ES101 읽어보기 *참고 1: ES_55 패치 필요, OpenJDK 마이그레이션 문서 참조* *참고 2: Tomcat 버전 확인- 아래의 "ICM 서버에서 Tomcat 버전 확인" 섹션을 참조하십시오.*	패치 - 12.6(1)_ES1 읽어보기
CTIOS		영향을 받지 않음	영향을 받지 않음	영향을 받지 않음	영향을 받지 않음
	ID	**11.6(1)**	**12.0(1)**	**12.5(1)**	**12.6(1)**
CVP	CSCwa47275	패치 - 11.6(1) ES16 추가 정보	패치 - 12.0(1)_ES10 읽어보기	패치 - 12.5(1)_ES25 읽어보기	패치 - 12.6(1)_ES9 읽어보기
VB	CSCwa47397	영향을 받지 않음	영향을 받지 않음	패치 - 12.5(1)_ES12 추가 정보	패치 - 12.6(1)_ES0 읽어보기 ** 2021년 12 29일에 게시 치 사용*
Call Studio	CSCwa54008	Callstudio_11.6_Log4j_fix 읽어보기	Callstudio_12.0(1)_Log4j_fix 읽어보기	Callstudio_12.5(1)_Log4j_fix 읽어보기	Callstudio_1)_Log4j_fix 읽어보기
Finesse	CSCwa46459	영향을 받지 않음	영향을 받지 않음	영향을 받지 않음	패치 - 12.6(1)_ES3 읽어보기
CUIC	CSCwa46525	영향을 받지 않음	영향을 받지 않음	영향을 받지 않음	패치 - 12.6(1)_ES0 읽어보기
라이브 데이터(LD)	CSCwa46810	패치 - 11.6.1_COP23 읽어보기	패치 - 12.0(1)_ES18 읽어보기	패치 - 12.5(1)_ES13 읽어보기	패치 - 12.6(1)_ES0 읽어보기
IDS		영향을 받지 않음	영향을 받지 않음	영향을 받지 않음	영향을 받지 않음
CUIC Co-res(CUIC-LD-IDS)	CSCwa46810	패치 - 11.6.1_COP23 읽어보기	패치 - 12.0(1)_ES18 읽어보기	패치 - 12.5(1)_ES13 읽어보기	패치 - 12.6(1)_ES0 읽어보기
CloudConnect	CSCwa51545			영향을 받지 않음	패치 - 12.6(1)_CC
ECE	CSCwa47392	영향을 받지 않음	패치 - 12.0(1)_ES6_ET2 읽어보기	패치 - 12.5(1)_ES3_ET2 읽어보기	패치 - 12.6(1)_ET2 읽어보기
CCMP	CSCwa47383	영향을 받지 않음	영향을 받지 않음	패치 - 12.5(1)_ES6	패치-12.6(1

				읽어보기	읽어보기
CCDM	CSCwa47383	영향을 받지 않음	영향을 받지 않음	패치 - 12.5(1) ES6 읽어보기	패치 - 12.6(1) ES3 읽어보기
구글 CCAI	Google에서 CACI 기능 집합에 영향을 미치지 않음				
Webex Experience Management(WxM)	WxM은 사용자 log4j를 수행하지 않으므로 솔루션이 영향을 받지 않습니다.				
고객 협업 플랫폼(CCP)	CSCwa47384	영향을 받지 않음	영향을 받지 않음	영향을 받지 않음	영향을 받지 않음

** 릴리스 날짜는 변경될 수 있으며 패치가 릴리스될 때까지 필요에 따라 업데이트됩니다.*

ICM 서버에서 Tomcat 버전 확인

1. ICM 서버(예: 라우터, 로거, PG 및 AW 서버)에서 "*<ICM HOME>\tomcat\bin\version.bat*" 파일을 실행하여 설치된 tomcat 버전을 확인합니다.
2. tomcat 버전이 **9.0.37 이상인** 경우 "CSCvv73307" 결함을 수정하려면 다음 단계를 수행합니다.
3. 서버에 ES_81 패치를 설치합니다. ICM 서버에 81보다 큰 ES가 있는 경우 먼저 해당 ES를 제거하십시오.

- 12.5(1)_ES81 패치 - 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. ES_81을 성공적으로 설치한 후 bat 파일 *"<ICM HOME>\tomcat\bin\version.bat"을* 실행하여 tomcat 버전을 다시 확인합니다.
5. Tomcat 버전은 1단계와 동일하게 유지되어야 합니다. 동일한 방식으로 원하는 모든 ES를 순차적으로 재설치하고 log4j 패치(예: ES_101)를 포함합니다.

자주 묻는 질문

Q.1 최신 정보로 문서를 얼마나 자주 수정합니까?

답변: 이 문서는 매일 검토되고 오전(미국 시간)에 업데이트됩니다.

Q.2 ICM 버전은 다음과 같습니다. (라우터, 로거, AW, PG) 10.x, 11.0(x), 11.5(x) 및 11.6(1)에 영향을 미칩니까?

답변: 이러한 버전은 log4j의 1.X 버전을 사용하므로 영향을 받지 않습니다.

> **참고:** 자문 테이블에는 유지 관리 중인 버전의 특정 버그가 나열됩니다. 강조 표시되지 않은 버전은 소프트웨어 유지 관리의 종료이며 검토용으로 고려되지 않습니다.

Q3 패치는 언제 릴리스됩니까?

답변: 권고 사항 테이블에는 패치가 릴리스되는 시기가 미정 날짜를 강조 표시합니다. 테이블이 사용 가능해지면 관련 링크로 업데이트됩니다.

Q.4 수정 준비가 될 때까지 구현할 수 있는 해결 방법

답변: 권장 사항은 PSIRT 권고 사항을 따르고 영향을 받는 버전에 대해 가능한 빨리 패치가 적용되도록 하는 것입니다.

Q.5 CUIC Standalone 11.6(1)은 log4j에 영향을 받지 않습니다. 그러나 ES의 Readme에 서버에 필요한 패치가 있다고 설명되어 있습니다. 이유는 무엇입니까?

대답: 이 ES는 log4j 수정 사항만 있는 독립형 ES가 아니며, 이 ES23은 모든 VOS 제품에 대해 우리가 가지고 있는 누적 ES입니다. 즉, 고객에게 어떤 시점에서든 사용 가능한 최신 누적 ES는 하나뿐입니다. Cu가 독립형 CUIC 11.6 ES 21(또는 그 이전)에 있고 ES22의 CUIC 결함 수정을 요구하는 이 시나리오를 가정해 보십시오. 이 경우 ES23을 설치해야 합니다(ES는 누적 버전이며 고객은 최신 버전의 ES만 사용 가능). 또한 이 log4j 결함은 ES Readme의 LD 결함 아래에 언급되어 있습니다. ES 설치 중에, 적용 가능한 구축에 따라 결함 수정이 설치됩니다(즉, ES 설치 전 독립형 CUIC /co-res CUIC/LD 적용 여부 확인).

Q.6 조직 보안 스캐너인 경우 어떤 조치를 취해야 합니까(예: Qualys)가 UCCE 제품을 패치한 후 CVE-2021-45105를 선택합니까?

답변: Cisco가 CVE-2021-45105를 검토했고 이 취약성의 영향을 받는 Cisco 제품 또는 클라우드 제품이 없다고 판단했으므로 어떠한 조치도 필요하지 않습니다. 이 정보는 자문 항목에서도 강조 표시되어 있습니다. Log4j 버전 2.16.0이 DDoS에 취약하려면 익스플로잇을 수행하려면 기본이 아닌 구성이 필요합니다. 즉, 공격자는 log4j 컨피그레이션 파일을 수동으로 수정해야 하며 UCCE 제품에서는 이 작업을 수행할 수 없으므로 CVE-2021-45105는 적용할 수 없습니다.

Q7. 1.2x 파일과 같은 시스템에 이전 Log4j ".jar" 파일이 표시되면 어떻게 해야 합니까?

답변: 롤백 프로세스가 중단되지 않도록 이전 파일을 유지하는 것이 좋습니다. 시스템에 이러한 파일의 비활성 버전이 있으면 구성 요소가 취약한 상태로 유지되지 않습니다.

그러나 기업에서 파일을 제거해야 하는 경우, 영향을 최소화하기 위해 프로덕션 단계를 구현하기 전에 Lab에서 원하는 프로세스를 테스트하는 것이 좋습니다. 또한 작업에 문제가 있을 경우 시스템을 복구할 수 있도록 백업 및 롤백 계획을 쉽게 만드는 것이 좋습니다.