Fehlerbehebung bei Apache Log4j-Schwachstellen in der Unified Contact Center Express-Lösung

Inhalt

Einleitung

In diesem Dokument werden die Auswirkungen der Apache Log4j-Schwachstelle auf die Cisco Contact Center Express (UCCX)-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 Express-Produktversion 12.5.x.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Apache gab im Dezember eine Schwachstelle in Log4j-Komponente bekannt. Sie wird häufig in der Cisco Unified Contact Center Express-Lösung verwendet, und Cisco ist aktiv an der Evaluierung der Produktpalette beteiligt, um zu überprüfen, was sicher ist und was davon betroffen ist.

Anmerkung: Weitere Informationen finden Sie unter Cisco Security Advisory - cisco-sa-apache-log4j

Dieses Dokument enthält weitere Informationen, sobald diese verfügbar sind.

Anwendung	Defekt-ID	11.6.(2)	12.0(1)	12.5(1)	12.5.1(SU1)
UCCX	Cisco Bug-ID CSCwa47388	Nicht betroffen	Nicht betroffen	Keine Behebung (siehe Hinweis)	12,5(1)_SU0 S03
CCP (Social Miner)		Nicht betroffen	Nicht betroffen	Nicht betroffen	12,5(1)_SU0 S03
WebEx Experience Management (WXM)		WxM verwendet log4j nicht, weshalb die Lösung nicht beeinträchtigt ist.			

Anmerkung: Die Reparatur für Kunden im 12.5-Zug darf nur für 12.5(1)SU1ES03 verfügbar sein. Kunden mit 12.5(1) müssen ein Upgrade auf 12.5(1)SU1 durchführen, um ES03 anzuwenden. Dies erfordert zwar ein Wartungsfenster, es beeinträchtigt jedoch nicht die Kompatibilität mit anderen Komponenten im Kundennetzwerk.

Häufige Fragen

F.1 Sind Finesse und CUIC ebenfalls betroffen und ist ihr unterschiedlicher Patch für sie?

Antwort: Finesse und CUIC sind in das UCCX-Softwarepaket integriert. Der Patch, der veröffentlicht werden soll, stellt somit das Fix für den gesamten UCCX-Server bereit.

Frage 2 Sind auch die UCCX-Versionen unter UCCX 11.6.2 betroffen?

Antwort: Nein. Diese Versionen sind als nicht beeinträchtigt gekennzeichnet.

Q.3 Wann werden Patches veröffentlicht?

Antwort: Der Beratungstabelle zeigt ein zaghaftes Datum für die Veröffentlichung der Patches. Die Tabelle sollte mit den entsprechenden Links aktualisiert werden.

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.

Frage 5 Wie oft wird das Dokument mit den neuesten Informationen überarbeitet?

Antwort: Das Dokument wird täglich überprüft und morgens (IST-Stunden) aktualisiert.

Q.6 Ist die CCX-Lösung mit Patches für die Schwachstelle CVE-2021-45105 erhältlich, da log4j eine neue, reparierte Version, d. h. 2.17.0, bereitstellt?

Antwort: Ja, der Patch 12.5(1)_SU01_ES03 besteht aus der Behebung der Schwachstelle CVE-2021-45105.