Begrijp de impact van Apache Log4j kwetsbaarheid in Cisco contactcenteroplossing

Inhoud

Inleiding

Dit document beschrijft de gevolgen van Apache Log4j kwetsbaarheid op de productlijn van Cisco Contact Center (UCCE).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Unified Contact Center productversie 11.6 en hoger.

Achtergrondinformatie

Apache kondigde onlangs een kwetsbaarheid aan in de component Log4j. Het wordt veel gebruikt in Cisco Contact Center-oplossing en Cisco is actief in de evaluatie van de productlijn om te controleren wat veilig is en wat wordt beïnvloed.

> **Opmerking:** Meer informatie is hier beschikbaar: [Cisco Security Advisories - cisco-sa-apache-log4j](#)

Dit document bevat meer informatie naarmate het beschikbaar wordt.

Toepassing	ID uitzetten	11.6.(2)	12.0(1)	12.5(1)	12.6(1)

UCCE/ICM	CSCwa47273	Patch - 11.6(2)_ES84 LeesMe	Patch - 12.0(1)_ES91 LeesMe	Patch - 12.5(1)_ES101 LeesMe *Opmerking 1: ES_55-pleister vereist, raadpleeg OpenJDK Migratiedoc* *Noot 2: Tomcat Versie check-refrein sectie "Tomcat Versie check op ICM servers" hieronder*	Patch - 12.6(1)_ES1 LeesMe
PCCE	CSCwa47274	Patch - 11.6(2)_ES84 LeesMe	Patch - 12.0(1)_ES91 LeesMe	Patch - 12.5(1)_ES101 LeesMe *Opmerking 1: ES_55-pleister vereist, raadpleeg OpenJDK Migratiedoc* *Noot 2: Tomcat Versie check-refrein sectie "Tomcat Versie check op ICM servers" hieronder*	Patch - 12.6(1)_ES1 LeesMe
CTIOS		Niet beïnvloed	Niet beïnvloed	Niet beïnvloed	Niet beïnvloed
Toepassing	**ID uitzetten**	**11.6(1)**	**12.0(1)**	**12.5(1)**	**12.6(1)**
CVP	CSCwa47275	Patch - 11.6(1) ES16 Leesmij	Patch - 12.0(1)_ES10 LeesMe	Patch - 12.5(1)_ES25 LeesMe	Patch - 12.6(1)_ES LeesMe
VVB	CSCwa47397	Niet beïnvloed	Niet beïnvloed	Patch - 12.5(1)_ES12 Leesmij	Patch - 12.6(1)_ES LeesMe ** gebruik va pleister, gepubliceer 29 decembe 2021*
Call Studio	CSCwa5408	Callstudio_11.6_Log4j_fix LeesMe	Callstudio_12.0(1)_Log4j_fix LeesMe	Callstudio_12.5(1)_Log4j_fix LeesMe	Callstudio_1)_Log4j_fix LeesMe
Finesse	CSCwa46459	Niet beïnvloed	Niet beïnvloed	Niet beïnvloed	Patch - 12.6(1)_ES LeesMe
CUIC	CSCwa46525	Niet beïnvloed	Niet beïnvloed	Niet beïnvloed	Patch - 12.6(1)_ES LeesMe
Levende gegevens (LD)	CSCwa46810	Patch - 11.6.1_COP23 LeesMe	Patch - 12.0(1)_ES18 LeesMe	Patch - 12.5(1)_ES13 LeesMe	Patch - 12.6(1)_ES LeesMe
IDS		Niet beïnvloed	Niet beïnvloed	Niet beïnvloed	Niet beïnvloed
CUIC-coders (CUIC-LD-IDS)	CSCwa46810	Patch - 11.6.1_COP23 LeesMe	Patch - 12.0(1)_ES18 LeesMe	Patch - 12.5(1)_ES13 LeesMe	Patch - 12.6(1)_ES LeesMe
CloudConnect	CSCwa51545			Niet beïnvloed	Patch - 12.6(1)_CC
ECE	CSCwa47392	Niet beïnvloed	Patch - 12.0(1)_ES6_ET2 LeesMe	Patch - 12.5(1)_ES3_ET2 LeesMe	Patch - 12.6(1)_ET LeesMe

CCMP	CSCwa47383	Niet beïnvloed	Niet beïnvloed	Patch - 12.5(1)_ES6 LeesMe	Patch-12.6(1)_ES3 LeesMe
CCDM	CSCwa47383	Niet beïnvloed	Niet beïnvloed	Patch - 12.5(1)_ES6 LeesMe	Patch - 12.6(1)_ES3 LeesMe
Google CCAI	Google-bevestigde CCAI-functieset is niet van invloed				
Webex Experience Management (WXM)	WxM gebruikt log4j niet en de oplossing is niet beïnvloed				
Customer Collaboration Platform (CCP)	CSCwa47384	Niet beïnvloed	Niet beïnvloed	Niet beïnvloed	Niet beïnvloed

** De datum van afgifte kan worden gewijzigd en zal zo nodig worden bijgewerkt tot de pleister is vrijgegeven*

Tomcat Versie controleren op ICM servers

1. Op ICM-servers, d.w.z. routers, loggers, PG- en AW-servers, controleren de versie van de geïnstalleerde tekst door middel van een "*<ICM HOME>\tomcat\bin\version.bat*"-bestand.
2. Als de versie van de tomcat **9.0.37 of hoger** is, voert u deze stappen uit om het defect "CSCv73307 te herstellen"
3. Installeer ES_81-pleister op de server. Indien er ES groter is dan 81 op de ICM server, zorg er dan voor dat deze ES's eerst worden verwijderd

- 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. Nadat ES_81 met succes is geïnstalleerd, bevestig de versie van de tekst opnieuw door het vleermuisbestand *"<ICM HOME>\tomcat\bin\version.bat" te* gebruiken
5. De versie van de Tomcat moet hetzelfde blijven als stap 1. Als hetzelfde doorgaat met het op ordelijke wijze opnieuw installeren van alle gewenste ES tot en met een log4j-pleister, d.w.z. ES_101

Vaak gestelde vragen

Vraag 1.1 Hoe vaak wordt het document met de meest recente informatie herzien?

Antwoord: Het document wordt dagelijks bekeken en 's morgens bijgewerkt

Q.2 zijn de ICM versies, d.w.z. (router, Logger, AW, PG) 10.x, 11.0(x), 11.5(x) en 11.6(1) beïnvloed?

Antwoord: Deze versies hebben geen invloed op de manier waarop ze de 1.X versie van log4j gebruiken.

> **Opmerking:** In de adviestabel worden specifieke insecten genoemd voor de in onderhoud zijnde versies. Versies die niet worden gemarkeerd, zijn het einde van software-onderhoud en worden niet in aanmerking genomen voor review.

Vraag 3 wanneer worden patches vrijgegeven?

Antwoord: In de adviestabel worden de voorlopige data voor de vrijgave van de patches aangegeven. De tabel wordt met de bijbehorende koppelingen bijgewerkt zodra deze beschikbaar worden.

Vraag 4. Enige werkronden die kunnen worden uitgevoerd totdat de oplossing klaar is?

Antwoord: De aanbeveling is om het advies van PSIRT te volgen en ervoor te zorgen dat patches zo snel mogelijk worden toegepast zodra ze voor de betrokken versies zijn vrijgegeven.

Q.5 CUIC Standalone 11.6(1) wordt niet beïnvloed door log4j, hoewel het leesmij van ES op de server een vereiste vlek geeft - waarom?

Antwoord: Dit ES is geen standalone ES met alleen log4j-oplossing, dit ES23 is een cumulatief ES zoals we zouden hebben voor elk VOS-product. Er is slechts één laatste en cumulatief ES beschikbaar voor de klant op elk tijdstip. Neem dit scenario in overweging, waarbij Cu zich in standalone CUIC 11.6 ES 21 (of eerder) bevindt en de CUIC defect fixes van ES22 vereist, in dat geval moeten ze nog steeds ES23 installeren (aangezien ES cumulatief zijn en alleen de laatste versie van ES beschikbaar is voor de klant). Bovendien wordt deze afwijking van log4j vermeld en vermeld onder LD-defect in de ES Readme. Tijdens de installatie van ES worden defectfixes geïnstalleerd op basis van de plaatsing zoals van toepassing (d.w.z. inzetcontrole wordt uitgevoerd of - standalone CUIC/co-res CUIC/LD vóór de installatie van ES en defectsfixes dienovereenkomstig worden toegepast)

Q.6 Welke acties onderneem ik als mijn organisaties beveiligingsscanner (voorbeeld: Qualys) pakt CVE-2021-45105 op nadat ik mijn UCCE Product heb gepatcheerd?

Antwoord: Er is geen actie nodig omdat Cisco CVE-2021-45105 heeft beoordeeld en heeft bepaald dat geen Cisco-producten of cloudproducten door deze kwetsbaarheid worden beïnvloed. Deze informatie is ook in het advies naar voren gebracht. Om DDoS kwetsbaar te kunnen maken, moet Log4j versie 2.16.0 een configuratie zonder standaardinstelling hebben om te kunnen profiteren. Dit betekent dat de aanvaller het logbestand4j handmatig moet wijzigen en dat dit niet mogelijk is in UCCE-producten. Daarom is CVE-2021-45105 niet van toepassing.

Q7. Wat doe ik als ik oudere logge4j ".jar" bestanden op mijn systeem zie zoals 1.2x bestanden?

Antwoord: Aanbevolen wordt de oude dossiers te laten liggen zodat het terugdraaiingsproces niet wordt doorbroken. Een inactieve versie van deze bestanden op het systeem laat de component niet kwetsbaar.

Als bedrijven echter willen dat de bestanden moeten worden verwijderd, wordt het sterk aangemoedigd om het gewenste proces in het laboratorium te testen voordat de productiestappen worden uitgevoerd om de impact tot een minimum te beperken. Het wordt ook aanbevolen om back-up- en terugdraaiplan handig te hebben om het systeem te herstellen in geval er problemen

zijn met de activiteit.