Entender o impacto da vulnerabilidade do Apache Log4j na solução Cisco Contact Center

Contents

Introduction

Este documento descreve o impacto da vulnerabilidade do Apache Log4j na linha de produtos do Cisco Contact Center (UCCE).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Produto Cisco Unified Contact Center versão 11.6 e posterior.

Informações de Apoio

O Apache anunciou recentemente uma vulnerabilidade no componente Log4j. Ele é amplamente usado na solução Cisco Contact Center e a Cisco está ativamente na avaliação da linha de produtos para verificar o que é seguro e o que é afetado.

> **Note**: Mais informações estão disponíveis aqui: Cisco Security Advisory - cisco-sa-apache-log4j

Este documento apresenta mais informações à medida que se torna disponível .

Aplicativo	ID do defeito	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 *Nota 1: Patch ES_55 necessário, consulte Documento de migração do OpenJDK* *Nota 2: Verificação da versão do Tomcat - Consulte a seção "Verificação da versão do Tomcat em servidores ICM" abaixo*	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 *Nota 1: Patch ES_55 necessário, consulte Documento de migração do OpenJDK* *Nota 2: Verificação da versão do Tomcat - Consulte a seção "Verificação da versão do Tomcat em servidores ICM" abaixo*	Patch - 12.6(1)_ES1 ReadMe
CTIOS		Não afetado	Não afetado	Não afetado	Não afetado
Aplicativo	**ID do defeito**	**11.6(1)**	**12.0(1)**	**12.5(1)**	**12.6(1)**
CVP	CSCwa47275	Patch - 11.6(1) ES16 Leiame	Patch - 12.0(1)_ES10 ReadMe	Patch - 12.5(1)_ES25 ReadMe	Patch - 12.6(1)_ES ReadMe
VVB	CSCwa47397	Não afetado	Não afetado	Patch - 12.5(1)_ES12 Leiame	Patch - 12.6(1)_ES ReadMe ** use patch publicado e de dezembr 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	Não afetado	Não afetado	Não afetado	Patch - 12.6(1)_ES ReadMe
CUIC	CSCwa46525	Não afetado	Não afetado	Não afetado	Patch - 12.6(1)_ES ReadMe
Dados ao vivo (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		Não afetado	Não afetado	Não afetado	Não afetado
Co-res CUIC (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			Não afetado	Patch - 12.6(1)_CC
ECE	CSCwa47392	Não afetado	Patch - 12.0(1)_ES6_ET2 ReadMe	Patch - 12.5(1)_ES3_ET2 ReadMe	Patch - 12.6(1)_ET ReadMe

CCMP	CSCwa47383	Não afetado	Não afetado	Patch - 12.5(1)_ES6 ReadMe	Patch-12.6(1)_ES3 ReadMe
CCDM	CSCwa47383	Não afetado	Não afetado	Patch - 12.5(1)_ES6 ReadMe	Patch - 12.6(1)_ES3 ReadMe
Google CCAI	O conjunto de recursos da CCAI confirmada pelo Google não é afetado				
Gerenciamento De Experiência Webex (WxM)	O WxM não usa log4j, portanto, a solução não é afetada				
Plataforma de colaboração com o cliente (CCP)	CSCwa47384	Não afetado	Não afetado	Não afetado	Não afetado

** As datas de liberação estão sujeitas a alterações e serão atualizadas conforme necessário até que o patch seja liberado*

Verificação de versão Tomcat em servidores ICM

1. Em servidores ICM, ou seja, roteadores, loggers, PG e servidores AW, verifique a versão do tomcat instalado executando o arquivo "*<ICM HOME>\tomcat\bin\version.bat*".
2. Se a versão do tomcat for **9.0.37 ou superior**, execute estas etapas para corrigir o defeito "CSCvv73307"
3. Instale o patch ES_81 no servidor. Se houver algum ES maior que 81 no servidor ICM, certifique-se primeiro de desinstalar o ES

- Patch 12.5(1)_ES81 - 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. Após a instalação bem-sucedida do ES_81, confirme novamente a versão tomcat executando o arquivo bat *"<ICM HOME>\tomcat\bin\version.bat"*
5. A versão Tomcat deve continuar a ser a mesma da etapa 1. Se a mesma opção continuar com a reinstalação ordenada de todos os ESs desejados e incluindo o patch log4j, isto é, ES_101

Perguntas frequentes

P.1 Com que frequência o documento é revisado com as informações mais recentes?

Resposta: O documento é revisado diariamente e atualizado de manhã (horas US)

P.2 As versões do ICM, por exemplo: (Roteador, Agente de Log, AW, PG) 10.x, 11.0(x), 11.5(x) e 11.6(1) afetados?

Resposta: Essas versões não são afetadas, pois usam a versão 1.X do log4j.

Note: A tabela de avisos lista bugs específicos para as versões que estão em manutenção.

As versões que não estão destacadas estão no fim da manutenção do software e não são consideradas para revisão.

P.3 Quando os patches são liberados?

Resposta: A tabela de avisos destaca as datas tentativas quando os patches são liberados. A tabela será atualizada com os links relacionados à medida que estiverem disponíveis.

P.4 Qualquer solução alternativa que possa ser implementada até que a correção esteja pronta?

Resposta: A recomendação é seguir a orientação da PSIRT e garantir que os patches sejam aplicados o mais rápido possível, quando lançados para as versões afetadas.

Q.5 CUIC autônomo 11.6(1) não é afetado pelo log4j, no entanto, o readme do ES afirma que é um patch necessário no servidor - por quê?

Resposta: Este ES não é um ES autônomo com somente correção log4j, este ES23 é um ES cumulativo como teríamos para qualquer produto VOS. ou seja, há apenas um ES mais recente e cumulativo disponível para o cliente a qualquer momento. Considere esse cenário, em que Cu está no CUIC 11.6 ES 21 independente (ou anterior) e está exigindo as correções de defeitos do CUIC de ES22, nesse caso eles ainda precisam instalar ES23 (pois ES são cumulativos e somente a versão mais recente de ES está disponível para o cliente). Além disso, este defeito de log4j é mencionado e listado sob defeito de LD no ES Readme. Durante a instalação ES, as correções de defeitos são instaladas com base na implantação conforme aplicável (isto é, verifica-se se o CUIC autônomo /co-res CUIC/LD antes da instalação ES e as correções de defeitos são aplicadas adequadamente)

P.6 Quais ações devo tomar se meu scanner de segurança da empresa (Exemplo: Qualys) atende o CVE-2021-45105 depois de corrigir meu produto UCCE?

Resposta: Nenhuma ação é necessária, pois a Cisco analisou o CVE-2021-45105 e determinou que nenhuma oferta de produtos ou nuvem da Cisco é afetada por essa vulnerabilidade. Essas informações também foram destacadas na assessoria. Para que a versão 2.16.0 do Log4j seja vulnerável a DDoS, é necessária uma configuração não padrão para a exploração. Isso significa que o invasor deve modificar manualmente o arquivo de configuração log4j e isso não é possível em produtos UCCE, portanto o CVE-2021-45105 não é aplicável.

P7. O que faço quando vejo arquivos Log4j ".jar" mais antigos no meu sistema, como arquivos 1.2x?

Resposta: A recomendação é deixar os arquivos antigos para que o processo de reversão não seja interrompido. Ter uma versão inativa desses arquivos no sistema não deixa o componente vulnerável.

No entanto, se a empresa exigir que os arquivos sejam removidos, é altamente recomendável testar o processo desejado em laboratório antes de implementar as etapas na produção para minimizar o impacto. Também é recomendável ter um plano de backup e reversão em mãos para recuperar o sistema caso haja problemas com a atividade.