Solucionar problemas de vulnerabilidade do Apache Log4j na solução Unified Contact Center Express

Contents

Introduction

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

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 Express versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Apache anunciou uma vulnerabilidade no componente Log4j em dezembro. Ele é amplamente usado na solução Cisco Unified Contact Center Express 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 no 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)	12.5.1(SU1)
UCCX	ID de bug da Cisco CSCwa47388	Não impactado	Não impactado	Sem Correção (consulte a Nota)	12,5(1)_SU0 S03
CCP (Social Miner)		Não impactado	Não impactado	Não impactado	12,5(1)_SU0 S03
Gerenciamento De Experiência Webex (WxM)		O WxM não usa log4j, portanto, a solução não é afetada.			

Note: A correção para os clientes no trem 12.5 deve estar disponível somente no 12.5(1)SU1ES03. Os clientes em 12.5(1) devem atualizar para 12.5(1)SU1 para aplicar ES03. Embora isso exija uma janela de manutenção, ela não quebra a compatibilidade com nenhum outro componente na rede do cliente.

Perguntas frequentes

P.1 O Finesse e o CUIC também são afetados e seu patch é diferente para eles?

Resposta: O Finesse e o CUIC estão integrados ao pacote de software UCCX. Assim, o patch a ser liberado fornecerá a correção para todo o UCCX Server.

P.2 As versões do UCCX são inferiores às do UCCX 11.6.2 também afetadas?

Resposta: Não. Essas versões são marcadas como não impactadas.

P.3 Quando os patches são liberados?

Resposta: A tabela de avisos destaca as datas tentativas quando os patches são liberados. A tabela deve ser atualizada com os links relacionados.

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.

P.5 Com que frequência o documento é revisado com as informações mais recentes?

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

P.6 Temos a solução CCX lançada com os patches para a vulnerabilidade CVE-2021-45105 já que o log4j forneceu uma nova versão fixa, ou seja, 2.17.0 ?

Resposta: Sim, o patch 12.5(1)_SU01_ES03 consiste na correção da vulnerabilidade CVE-2021-45105.