

# Corrigir vulnerabilidades mostradas no endpoint seguro

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

---

## Introdução

Este documento descreve como verificar a pontuação de risco da Cisco para endpoints e aplicar correções.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Console Cisco Secure Endpoint

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Endpoint Console v5.4.2025030619

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Problema

A Pontuação de Risco de Segurança da Cisco é representada em uma escala de 0 a 100. Ela quantifica o risco de uma vulnerabilidade observando a gravidade técnica e como os invasores do mundo real estão aproveitando a vulnerabilidade de forma selvagem.

Verifique a pontuação de risco de segurança da Cisco para endpoints e aplique a correção

sugerida.

## Solução

1- Para examinar a pontuação de risco de segurança da Cisco, navegue para Gerenciamento > Computadores e selecione Pontuação de Risco de Segurança da Cisco mostrada:



2- Você vê a lista de computadores. Expanda as informações do computador que deseja verificar e clique em Cisco Security Risk Score number exibido como mostrado:

Connector Version	T 1.14.0.1017 <a href="#">Show download URL</a>	Internal IP	[REDACTED]
Install Date	2025-03-22 07:55:47 UTC	External IP	[REDACTED]
Connector GUID	[REDACTED]	Last Seen	2025-03-25 10:48:59 UTC
BP Signature Version	48168	BP Signature Last Updated	2025-03-04 07:01:29 UTC
Definition Version	ClamAV Linux-Fall (daily.evd: 27577, main.evd: 62, bytecode.evd: 325)	Definitions Last Updated	2025-03-14 11:09:55 UTC
Update Server	clam-defs.lamp.cisco.com	Cisco Security Risk Score	100 (Updated: 2025-03-25 09:31:00 UTC)

Take Forensic Snapshot View Snapshot Investigate in Orbital 4 Events Device Trajectory Diagnostics View Changes

3- Você vê uma lista de CVEs que afetam o endpoint. Clique em Corrigir disponível como mostrado abaixo:

Overview	Vulnerabilities
<b>100</b> / 100 CVSS 3.1: 8.8 	<b>CVE-2023-4863</b> Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical) <a href="#">Fix Available</a>
<b>100</b> / 100 CVSS 3.1: 2.5 	<b>CVE-2023-50387</b> Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6440, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "Day/Trap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records. <a href="#">Fix Available</a>
<b>100</b> / 100 CVSS 3.1: 8.8 	<b>CVE-2023-5217</b> Heap buffer overflow in vpl encoding in libps in Google Chrome prior to 117.0.5938.132 and libps 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) <a href="#">Fix Available</a>
<b>100</b> / 100 CVSS 3.1: 8.8 	<b>CVE-2024-4347</b>

4- Aqui você vê as correções sugeridas para o CVE listado como mostrado abaixo:

## Vulnerability Fixes ✕

CVE-2023-4863

100 / 100  
 CVSS 3.1: 8.8

Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)

**Fixed By:**

- [USN-6368-1](#)

Close



Note: Se não houver correções disponíveis, entre em contato com o TAC.

---

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.