

# Correction des vulnérabilités affichées sur Secure Endpoint

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

---

## Introduction

Ce document décrit comment vérifier le score de risque Cisco pour les terminaux et appliquer les correctifs.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Console Cisco Secure Endpoint

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Console de terminal sécurisé v5.4.2025030619

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Problème

Le score des risques de sécurité Cisco est représenté sur une échelle de 0 à 100. Il quantifie le risque d'une vulnérabilité en examinant la gravité technique et la manière dont les pirates du monde réel exploitent la vulnérabilité dans la nature.

Vérifiez le score des risques de sécurité Cisco pour les terminaux et appliquez le correctif suggéré.

# Solution

1- Pour examiner le score des risques de sécurité Cisco, accédez à Gestion > Ordinateurs et sélectionnez Score des risques de sécurité Cisco affiché :



2- Vous voyez la liste des ordinateurs. Développez les informations relatives à l'ordinateur que vous souhaitez vérifier et cliquez sur Cisco Security Risk Score number affiché comme suit :

Connector Version	1.24.0.1017 <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	2025-03-15 10:48:58 UTC
BP Signature Version	48168	BP Signature Last Updated	2025-03-04 07:01:29 UTC
Definition Version	ClamAV Linux-Full (daily.cvd: 27577, main.cvd: 62, bytecode.cvd: 325)	Definitions Last Updated	2025-03-14 11:09:55 UTC
Update Server	clam-defs.lamp.cisco.com	Cisco Security Risk Score	100 (Updated: 2025-03-15 09:31:00 UTC)

[Take Forensic Snapshot](#) [View Snapshot](#) [Investigate in Orbital](#) [Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

3- Vous voyez la liste des CVE affectant le terminal. Cliquez sur Fix Available comme indiqué ci-dessous :

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, 6449, 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- Ici, vous voyez les correctifs suggérés pour le CVE répertorié comme suit :

## Vulnerability Fixes ✕

# CVE-2023-4863

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](#)

**100** / 100

CVSS 3.1: 8.8

Close



Remarque : En l'absence de correctifs, contactez le TAC.

---

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.