

# Correggi le vulnerabilità mostrate sull'endpoint sicuro

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

---

## Introduzione

In questo documento viene descritto come controllare il punteggio di rischio di Cisco per gli endpoint e applicare le correzioni.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Endpoint console

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Endpoint Console v5.4.2025030619

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Problema

Il punteggio di rischio per la sicurezza di Cisco è rappresentato su una scala da 0 a 100. Esso quantifica il rischio di una vulnerabilità analizzando la gravità tecnica e il modo in cui gli aggressori del mondo reale stanno sfruttando la vulnerabilità allo stato brado.

Controllare il punteggio Cisco Security Risk per gli endpoint e applicare la correzione suggerita.

# Soluzione

1- Per esaminare il punteggio dei rischi per la sicurezza di Cisco, selezionare Gestione > Computer e selezionare il punteggio dei rischi per la sicurezza di Cisco mostrato:



2- Viene visualizzato l'elenco dei computer. Espandere le informazioni sul computer che si desidera controllare e fare clic sul numero del punteggio di rischio per la sicurezza Cisco visualizzato come mostrato:

Connector Version	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-Full (daily.evd: 27537, 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 09:39:00 UTC)

[Take Forensic Snapshot](#) [View Snapshot](#) [Investigate in Orbital](#) [4 Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

3- Viene visualizzato l'elenco dei CVE che hanno effetto sull'endpoint. Fare clic su Correggi disponibile come illustrato di seguito:

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 libpwa in Google Chrome prior to 117.0.5938.132 and libpwa 1.3.3 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- Di seguito sono elencate le correzioni suggerite per il CVE:

## Vulnerability Fixes ✕

CVE-2023-4863

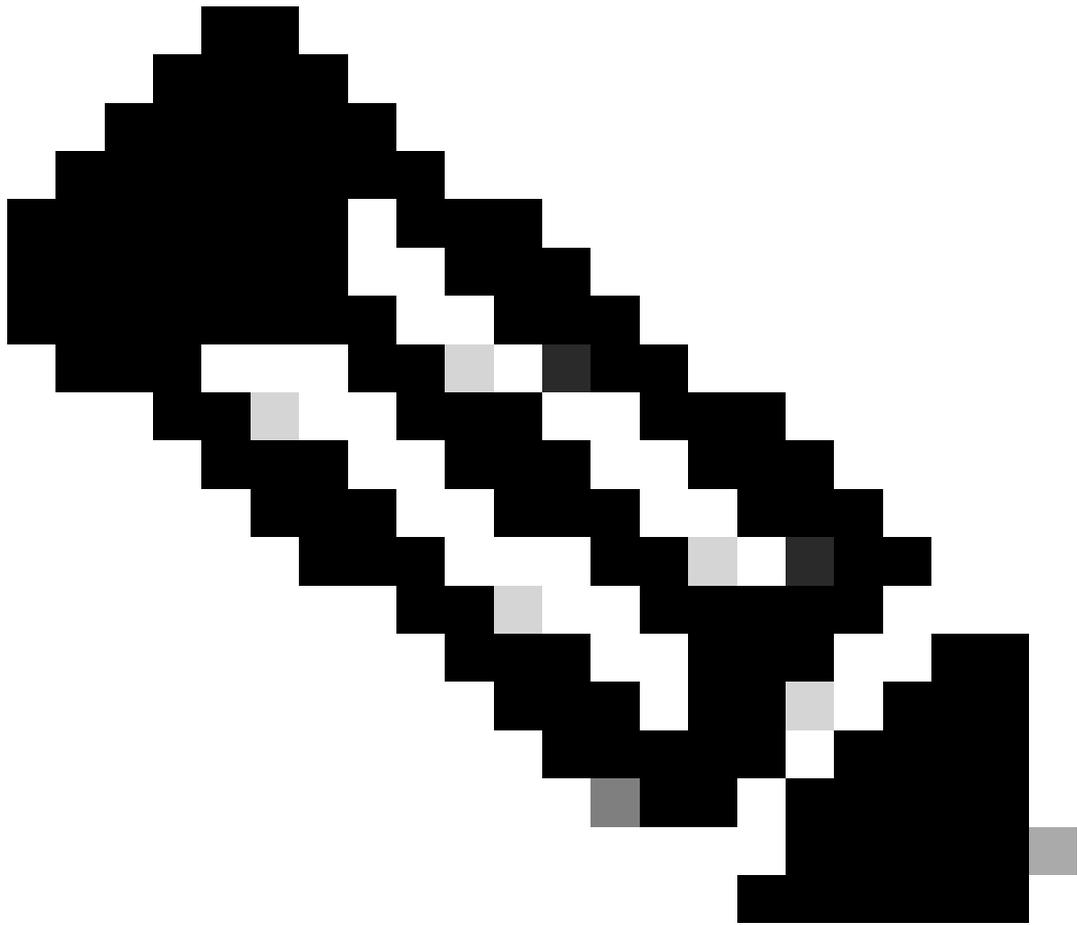
100 / 100  
 CVSS 3.1: 8.8

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



Nota: Se non sono disponibili correzioni, contattare TAC.

---

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).