

Solucione las vulnerabilidades mostradas en un terminal seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

Introducción

Este documento describe cómo verificar la puntuación de riesgo de Cisco para terminales y aplicar correcciones.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- consola de Cisco Secure Endpoint

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Secure Endpoint Console v5.4.2025030619

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

La puntuación de riesgos de seguridad de Cisco se representa en una escala del 0 al 100. Cuantifica el riesgo de una vulnerabilidad observando la gravedad técnica y el modo en que los atacantes reales aprovechan la vulnerabilidad de forma natural.

Compruebe la puntuación de riesgos de seguridad de Cisco para los terminales y aplique la

corrección sugerida.

Solución

1- Para ver la puntuación de riesgos de seguridad de Cisco, navegue hasta Administración > Equipos y seleccione la puntuación de riesgos de seguridad de Cisco que se muestra:



2- Verá la lista de ordenadores. Expanda la información del equipo que desea comprobar y haga clic en el número de Cisco Security Risk Score que se muestra como se muestra:

Connector Version	T 1.14.0.1017 Show download URL	Internal IP	[Redacted]
Install Date	2025-03-22 07:55:47 UTC	External IP	[Redacted]
Connector GUID	[Redacted]	Last Seen	2025-03-15 10:48:59 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: 2025-03-15 09:31:00 UTC)

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

3- Verá una lista de CVE que afectan al terminal. Haga clic en Fix Available como se muestra a continuación:

Overview	Vulnerabilities
<p>100 / 100</p> <p>CVSS 3.1: 8.8</p> <p>000</p>	<p>CVE-2023-4863</p> <p>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)</p> <p>Fix Available</p>
<p>100 / 100</p> <p>CVSS 3.1: 2.5</p> <p>00</p>	<p>CVE-2023-50387</p> <p>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.</p> <p>Fix Available</p>
<p>100 / 100</p> <p>CVSS 3.1: 8.8</p> <p>0</p>	<p>CVE-2023-5217</p> <p>Heap buffer overflow in vpl encoding in libvpx in Google Chrome prior to 117.0.5938.132 and libvpx 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)</p> <p>Fix Available</p>
<p>100 / 100</p>	<p>CVE-2024-4347</p>

4- Aquí puede ver las correcciones sugeridas para el CVE que se muestran a continuación:

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)

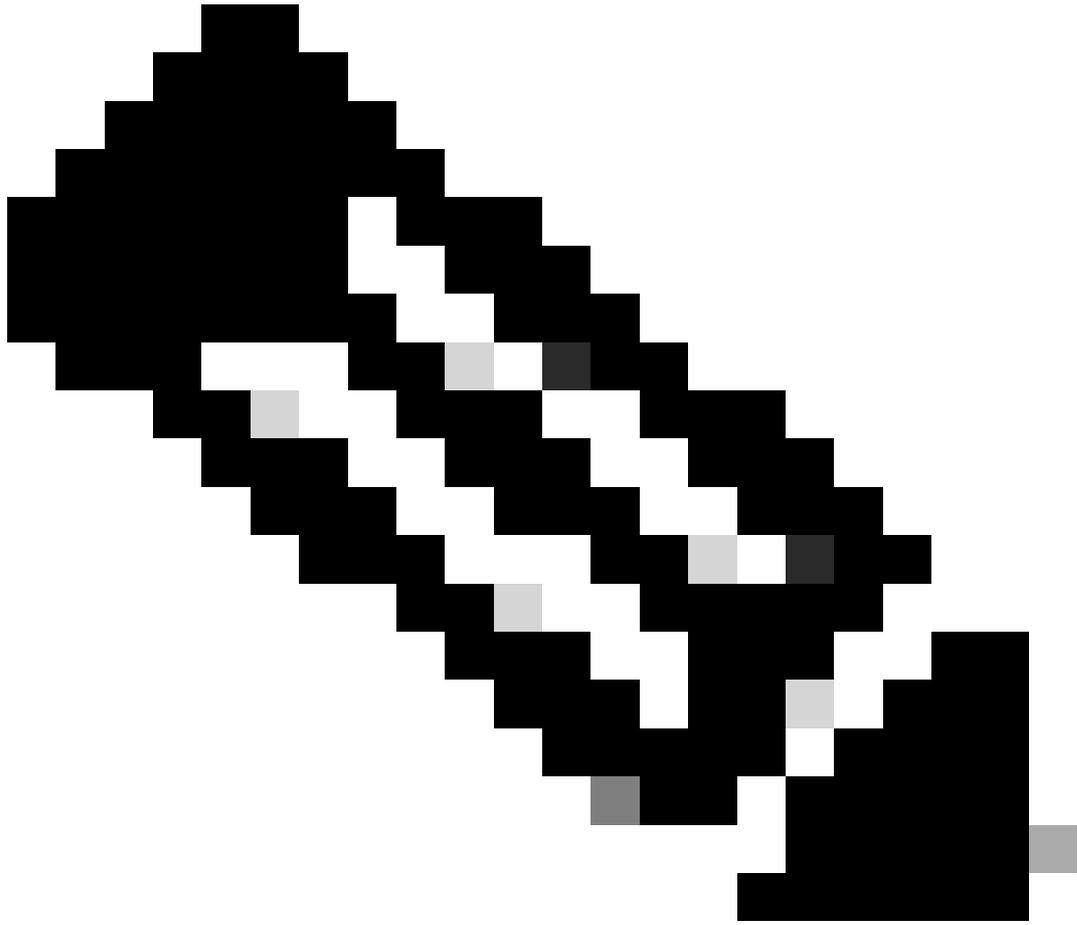
Fixed By:

- [USN-6368-1](#)

100 / 100

CVSS 3.1: 8.8

[Close](#)



Nota: Si no hay soluciones disponibles, póngase en contacto con el TAC.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).