Fix Vulnerabilities Shown on Secure Endpoint

Contents

Introduction

This document describes how to check Cisco risk score for endpoints and apply fixes.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Endpoint console

Components Used

The information in this document is based on these software versions:

- Secure Endpoint Console 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. If your network is live, ensure that you understand the potential impact of any command.

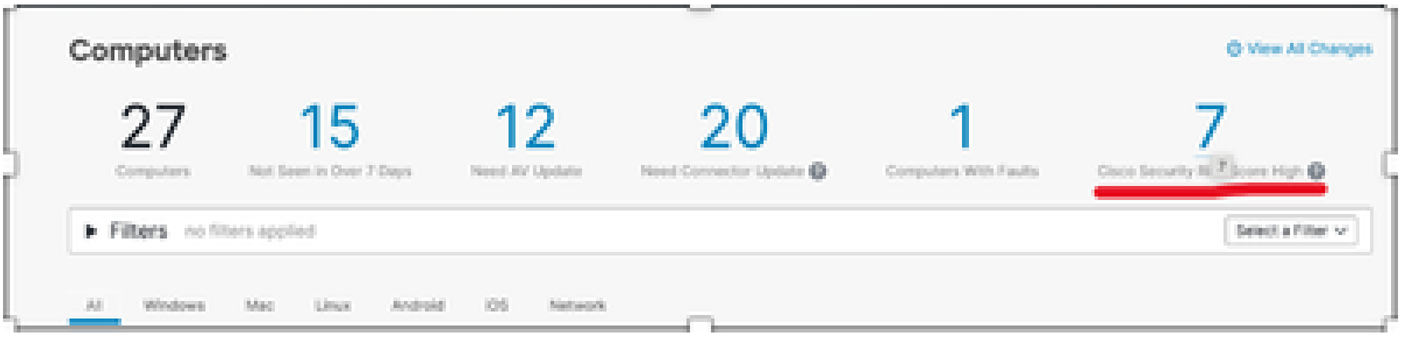
Problem

The Cisco Security Risk Score is represented on a scale from 0-100. It quantifies the risk of a vulnerability by looking at the technical severity and how real-world attackers are leveraging the vulnerability in the wild.

Check the Cisco Security Risk score for endpoints and apply suggested fix.

Solution

1- To look into the Cisco Security risk score, navigate to **Management > Computers and select Cisco Security Risk Score** shown:



Computers

⚙ View All Changes

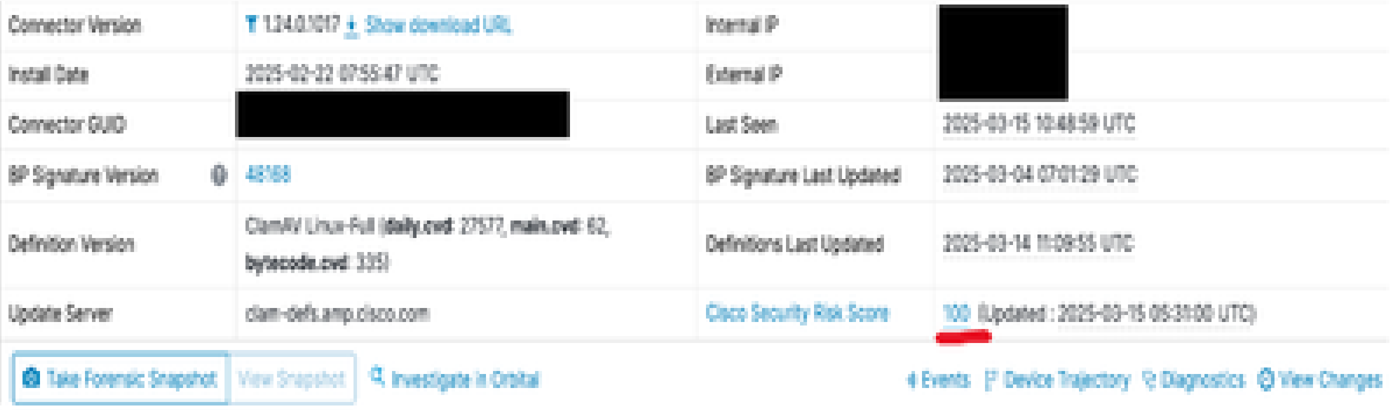
27	15	12	20	1	7
Computers	Not Seen In Over 7 Days	Need AV Update	Need Connector Update	Computers With Faults	Cisco Security Risk Score High

▶ Filters no filters applied

Select a Filter ⌄

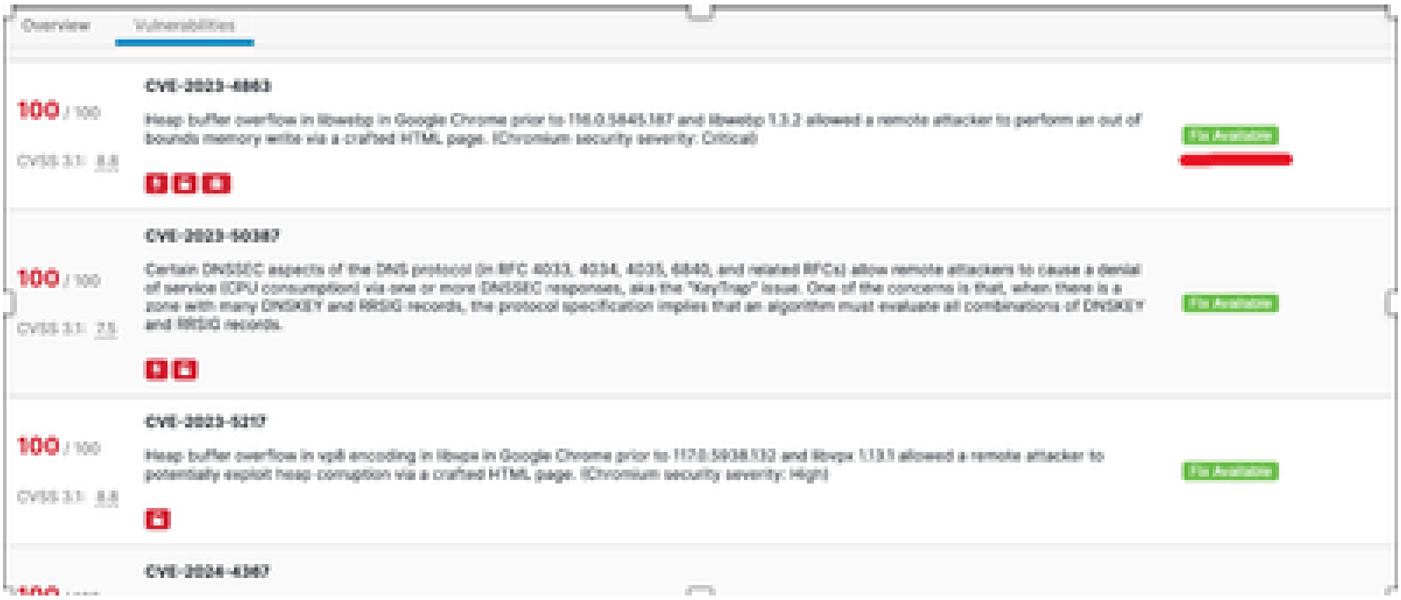
All Windows Mac Linux Android iOS Network

2- You see the list of computers. Expand the computer information you want to check and click **Cisco Security Risk Score number** displayed as shown:



Connector Version	1.24.0.1017 Show download URL	Internal IP	[redacted]
Install Date	2025-02-22 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-Full (**daily.cvd**: 27577, **main.cvd**: 62, **bytecode.cvd**: 335)	Definitions Last Updated	2025-03-14 11:09:55 UTC
Update Server	clam-defs.amp.cisco.com	Cisco Security Risk Score	100 (Updated : 2025-03-15 05:31:00 UTC)

3- You see list of CVE’s affecting the endpoint. Click **Fix Available** as shown below:



100 / 100 CVSS 3.1: 8.8

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)

Fix Available

100 / 100 CVSS 3.1: 7.5

CVE-2023-50387

Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" 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.

Fix Available

100 / 100 CVSS 3.1: 8.8

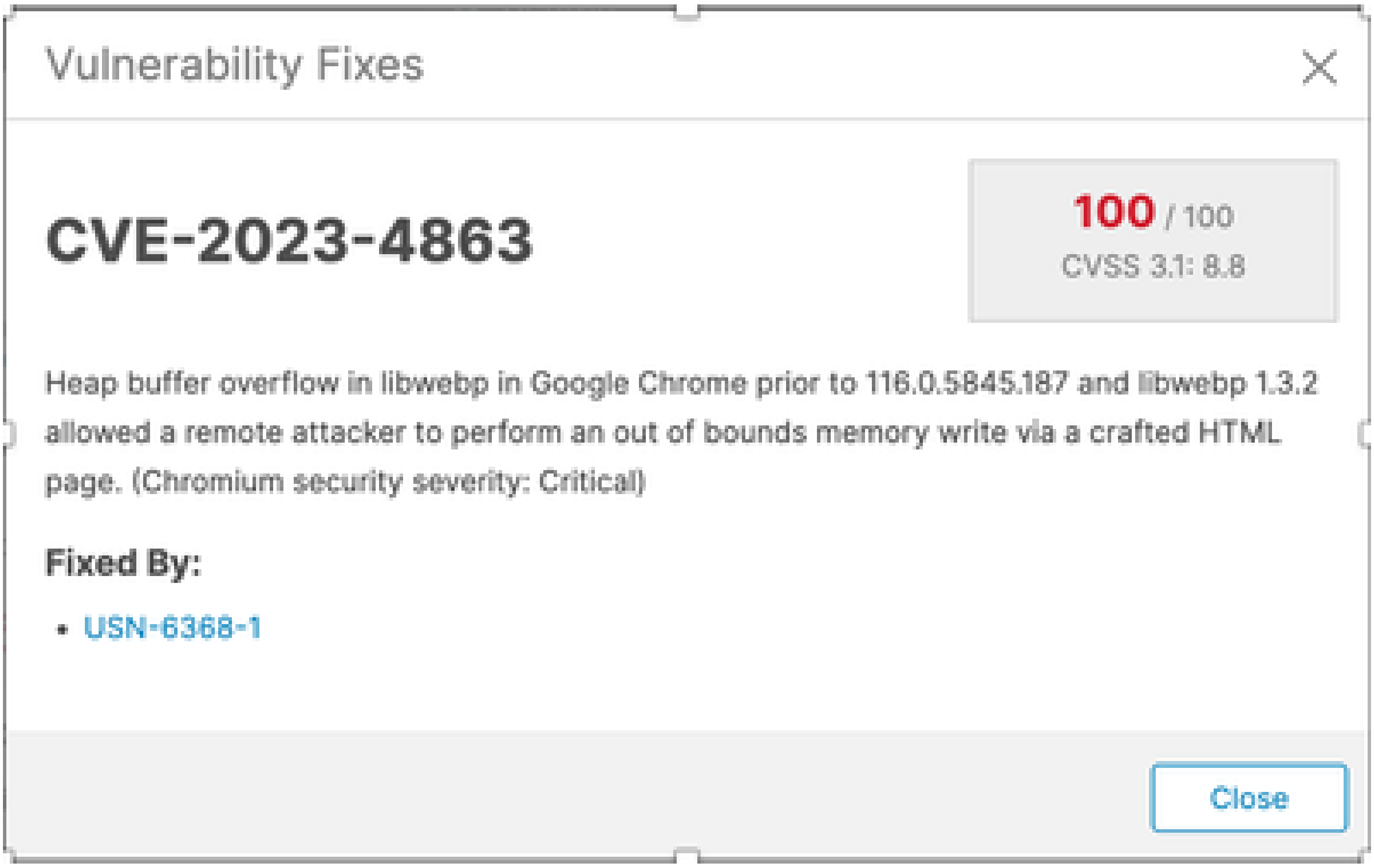
CVE-2023-5217

Heap buffer overflow in vp8 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)

Fix Available

CVE-2024-4367

4- Here you see the suggested fixes for the CVE listed as shown below:



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

Note: If there are no fixes available, contact TAC.