

# Fix Vulnerabiliteiten weergegeven op Secure Endpoint

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

---

## Inleiding

Dit document beschrijft hoe u de Cisco-risicoscore voor endpoints kunt controleren en oplossingen kunt toepassen.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Endpoint-console

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Endpoint console v5.4.2025030619

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

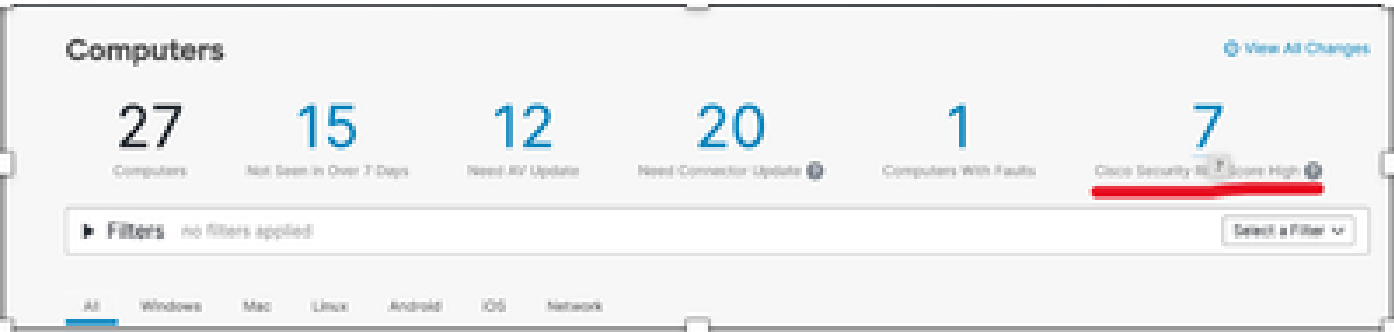
## Probleem

De Cisco Security Risk Score wordt weergegeven op een schaal van 0-100. Hij kwantificeert het risico van een kwetsbaarheid door te kijken naar de technische ernst en hoe echte aanslagplegers de kwetsbaarheid in het wild benutten.

Controleer de Cisco Security Risk score voor endpoints en pas de voorgestelde oplossing toe.

# Oplossing

1- Als u de Cisco Security Risk Score wilt bekijken, navigeert u naar Management > Computers en selecteert u de getoonde Cisco Security Risk Score:



2- Je ziet de lijst met computers. Breid de computerinformatie uit die u wilt controleren en klik op het Cisco Security Risk Score-nummer dat wordt weergegeven zoals:

|                                                                                                                                       |                                                                       |                           |                                        |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------|----------------------------------------|
| Connector Version                                                                                                                     | 1.24.0.1017 <a href="#">Show download URL</a>                         | Internal IP               |                                        |
| Install Date                                                                                                                          | 2025-03-22 07:55:47 UTC                                               | External IP               |                                        |
| Connector GUID                                                                                                                        |                                                                       | 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.cvd: 27572, main.cvd: 62, bytecode.cvd: 325) | Definitions Last Updated  | 2025-03-14 11:09:55 UTC                |
| Update Server                                                                                                                         | clam-defs.amp.cisco.com                                               | Cisco Security Risk Score | 100 (Updated: 2025-03-25 09:39:00 UTC) |
| <div>Take Forensic Snapshot View Snapshot Investigate in Orbital</div> <div>4 Events Device Trajectory Diagnostics View Changes</div> |                                                                       |                           |                                        |

3- U ziet een lijst met CVE' s die het eindpunt beïnvloeden. Klik op Fix Available (Beschikbare reparaties) zoals hieronder weergegeven:

| Overview                          | Vulnerabilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 100 / 100<br>CVSS 3.1: 8.8<br>■■■ | <b>CVE-2023-4863</b><br>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)<br><a href="#">Fix Available</a>                                                                                                                                                                                                         |
| 100 / 100<br>CVSS 3.1: 7.5<br>■■  | <b>CVE-2023-50387</b><br>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 "DayTrip" 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.<br><a href="#">Fix Available</a> |
| 100 / 100<br>CVSS 3.1: 8.8<br>■   | <b>CVE-2023-5217</b><br>Heap buffer overflow in vpl encoding in libvpx in Google Chrome prior to 117.0.5938.532 and libvpx 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)<br><a href="#">Fix Available</a>                                                                                                                                                                                                |
| 100 / 100<br>CVSS 3.1: 8.8<br>■■■ | <b>CVE-2024-4347</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

4- Hier ziet u de voorgestelde fixes voor de CVE zoals hieronder weergegeven:

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



Opmerking: Als er geen oplossingen beschikbaar zijn, neemt u contact op met TAC.

---

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.