

Beheben von Sicherheitslücken auf sicheren Endgeräten

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Cisco Risikoeinschätzung für Endgeräte überprüfen und entsprechende Korrekturen vornehmen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Endpoint-Konsole

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Endpoint Console v5.4.2025030619

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

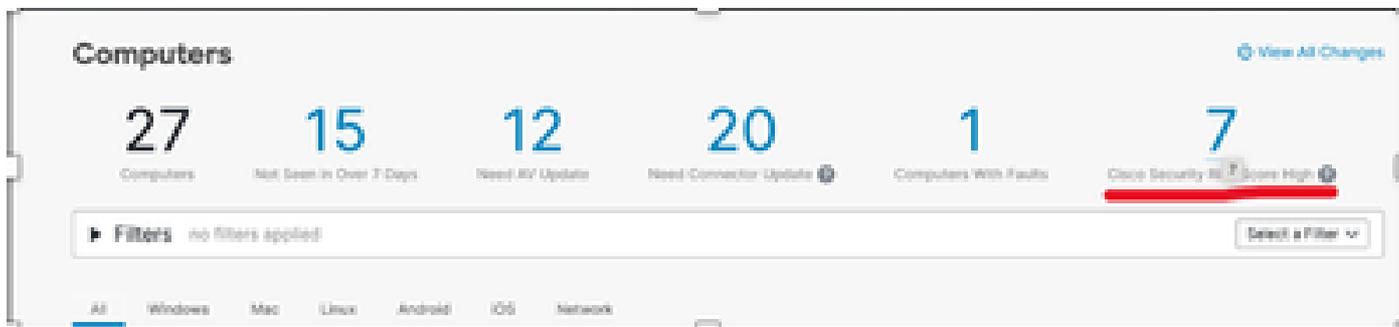
Der Cisco Security Risk Score wird auf einer Skala von 0 bis 100 dargestellt. Er quantifiziert das Risiko einer Schwachstelle, indem er den technischen Schweregrad und die Art und Weise, wie Angreifer diese Schwachstelle in freier Wildbahn ausnutzen, misst.

Überprüfen Sie die Cisco Sicherheitsrisikobewertung für Endgeräte, und wenden Sie die

empfohlene Korrektur an.

Lösung

1- Um die Cisco Sicherheitsrisikobewertung zu überprüfen, navigieren Sie zu Management > Computers, und wählen Sie die angezeigte Cisco Sicherheitsrisikobewertung aus:



2- Sie sehen die Liste der Computer. Erweitern Sie die Computerinformationen, die Sie überprüfen möchten, und klicken Sie auf Cisco Security Risk Score number (Cisco Sicherheitsrisiko-Punktzahl), die wie folgt angezeigt wird:

Connector Version	1.14.0.1017 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.ver: 27577, main.ver: 62, bytecode.ver: 329)	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 09:39:00 UTC)

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

3- Es wird eine Liste der CVEs angezeigt, die sich auf das Endgerät auswirken. Klicken Sie wie folgt auf Fix Available:

Overview	Vulnerabilities
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: 2.5 	CVE-2023-50387 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 "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 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) Fix Available
100 / 100 CVSS 3.1: 8.8 	CVE-2024-4347

4- Hier sehen Sie die vorgeschlagenen Korrekturen für den CVE, wie unten gezeigt:

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



Anmerkung: Falls keine Korrekturen verfügbar sind, wenden Sie sich an das TAC.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.