

セキュアエンドポイントに表示される脆弱性の修正

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

はじめに

このドキュメントでは、エンドポイントのシスコリスクスコアを確認し、修正を適用する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpointコンソール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- セキュアエンドポイントコンソールv5.4.2025030619

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

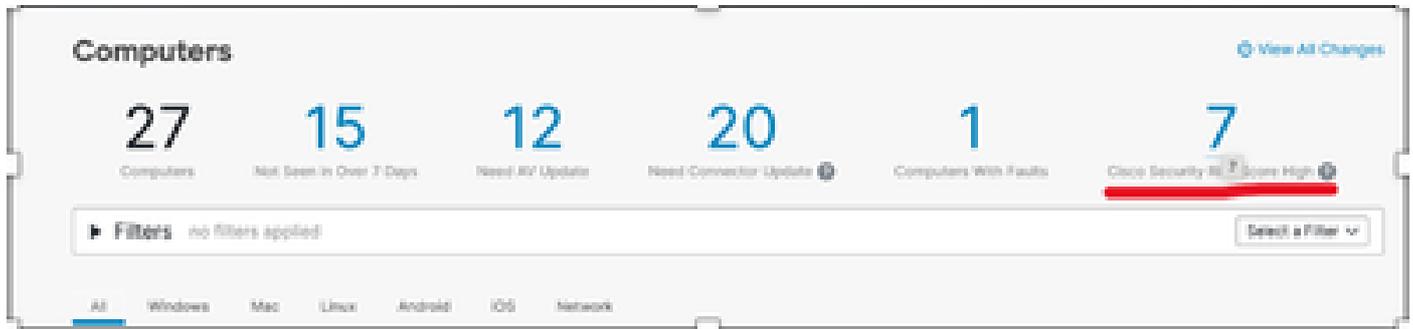
問題

シスコセキュリティリスクスコアは0 ~ 100の範囲で表されます。また、技術的な重大度と、実際の攻撃者がその脆弱性をどのように利用しているかを調べることで、脆弱性のリスクを定量化します。

エンドポイントのシスコセキュリティリスクスコアを確認し、推奨される修正を適用します。

解決方法

1- Cisco Securityリスクスコアを確認するには、Management > Computersに移動して、次に示すCisco Security Risk Scoreを選択します。



2 – コンピュータのリストが表示されます。確認するコンピュータ情報を展開し、次に示すように表示されるCisco Security Risk Score numberをクリックします。

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	2025-02-15 10:48:58 UTC
BP Signature Version	48168	BP Signature Last Updated	2025-02-04 07:01:29 UTC
Definition Version	ClamAV Linux-Full (daily.cvd: 27577, main.cvd: 62, bytecode.cvd: 325)	Definitions Last Updated	2025-02-14 11:09:55 UTC
Update Server	clam-defs.lamp.cisco.com	Cisco Security Risk Score	100 (Updated: 2025-02-15 09:31:00 UTC)

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

3 – エンドポイントに影響を与えるCVEのリストが表示されます。次に示すように、Fix Availableをクリックします。

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, 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. Fix Available
100 / 100 CVSS 3.1: 8.8 	CVE-2023-5217 Heap buffer overflow in vpl encoding in libps in Google Chrome prior to 117.0.5938.132 and libps 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- CVEの推奨される修正は次のとおりです。

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)

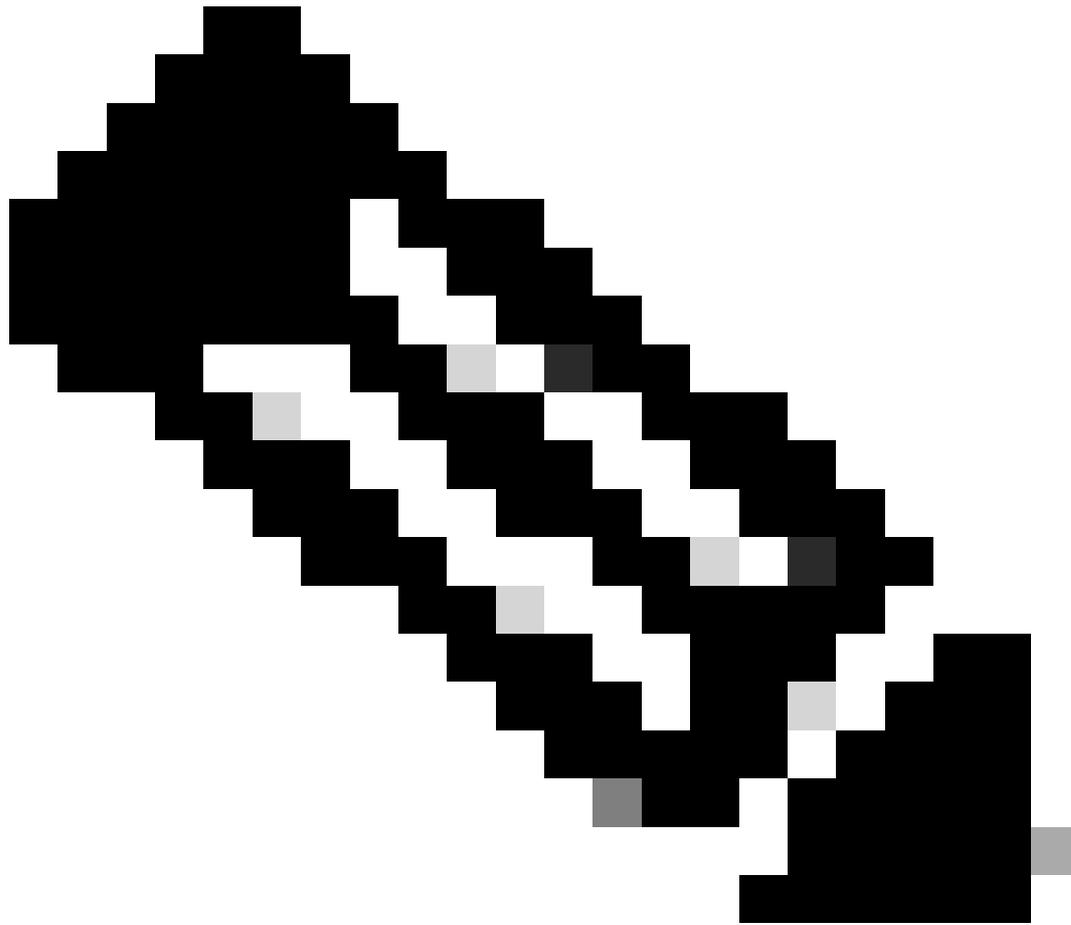
Fixed By:

- [USN-6368-1](#)

100 / 100

CVSS 3.1: 8.8

[Close](#)



注：利用可能な修正がない場合は、TACにお問い合わせください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。