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

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

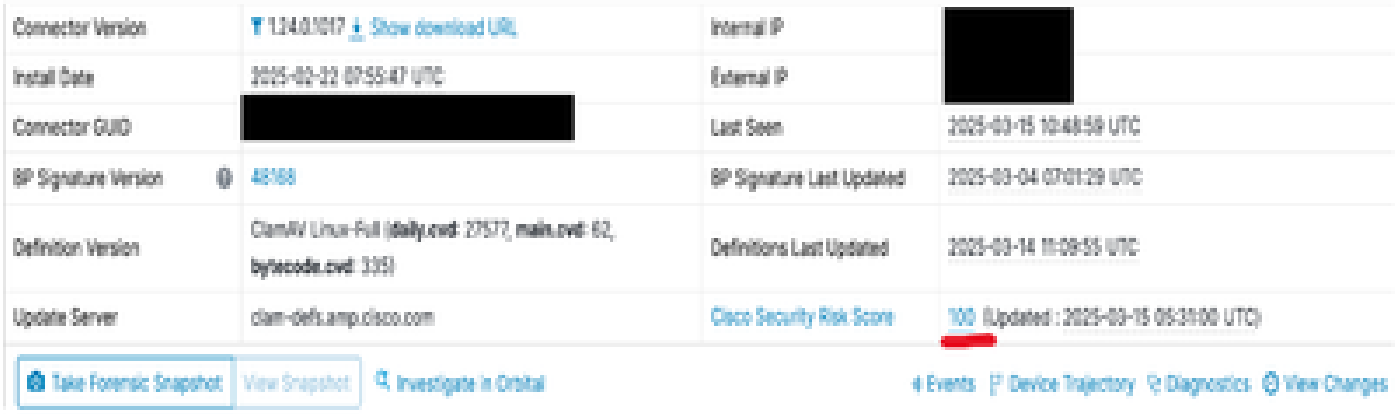
シスコセキュリティリスクスコアは0 ~ 100の範囲で表されます。また、技術的な重大度と、実際の攻撃者がその脆弱性をどのように利用しているかを調べることで、脆弱性のリスクを定量化します。

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

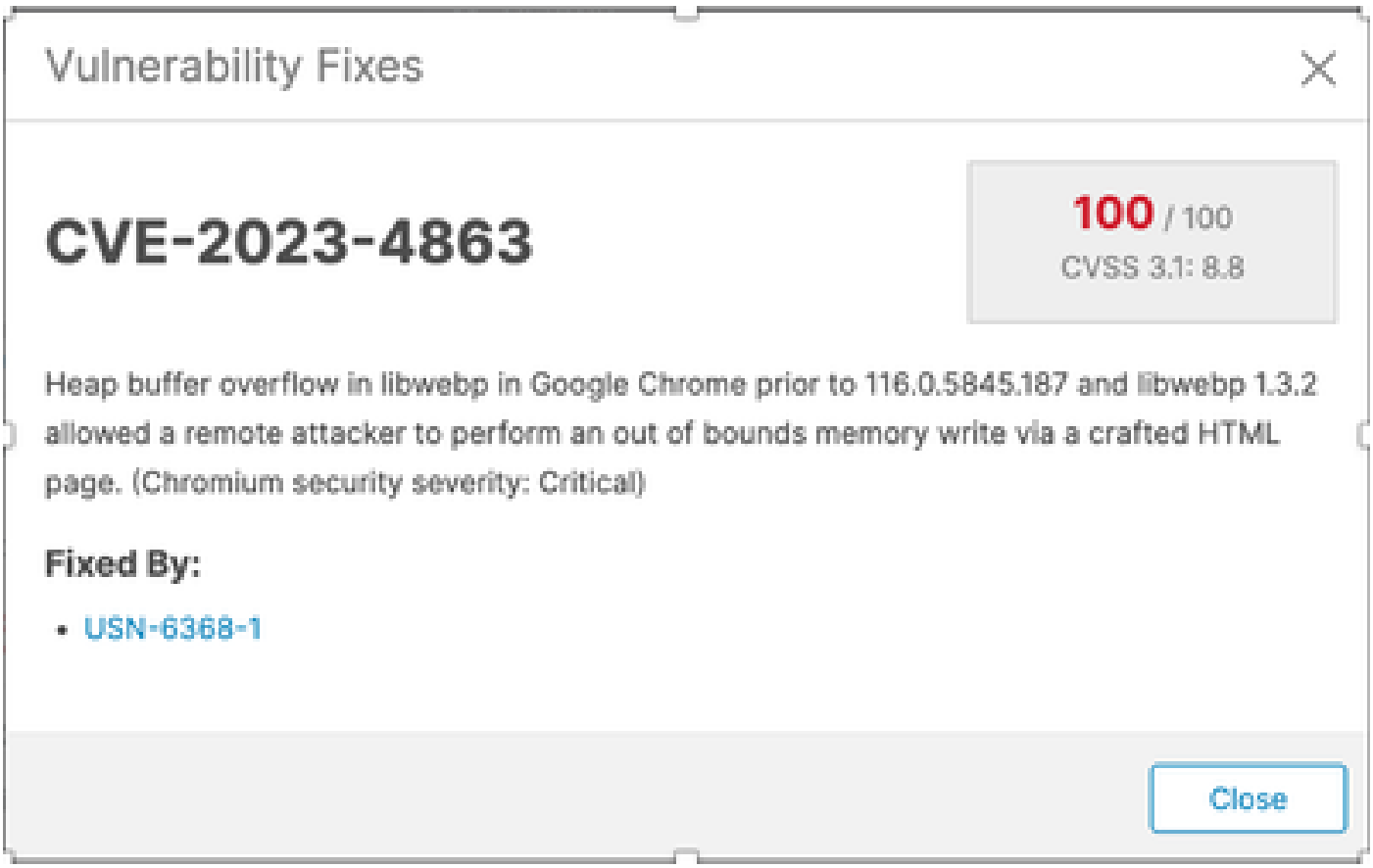
1- Cisco Securityリスクスコアを確認するには、Management > Computersに移動して、次に示すCisco Security Risk Scoreを選択します。

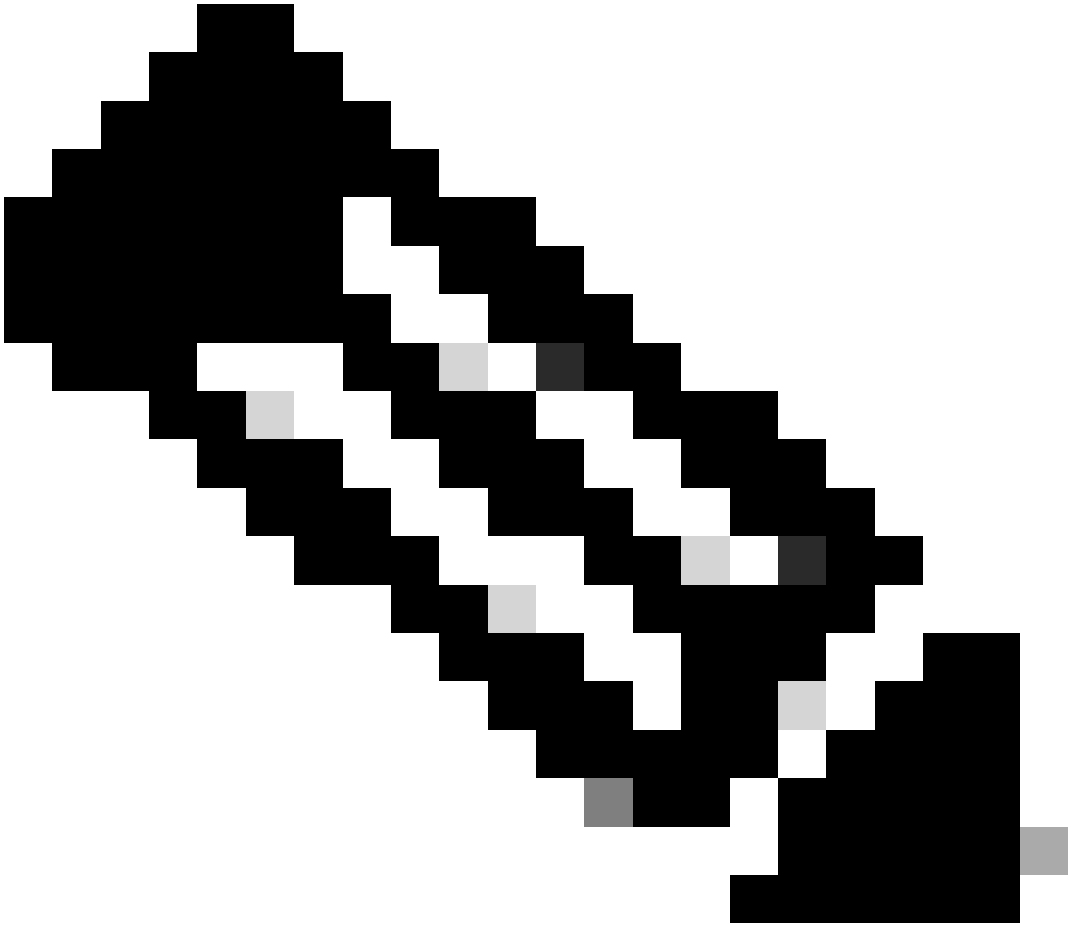
2 – コンピュータのリストが表示されます。確認するコンピュータ情報を展開し、次に示すように表示されるCisco Security Risk Score numberをクリックします。



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。

4- CVEの推奨される修正は次のとおりです。





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。