包括ルートCAにフラグを付けるセキュリティツールを解決する

内容

はじめに

このドキュメントでは、セキュリティ監査ツールによって包括ルートCAデジタル証明書にリスクとしてフラグが付けられる理由について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco UmbrellaセキュアWebゲートウェイ(SWG)に基づくものです。

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。

概要

Umbrellaインフラストラクチャのスキャンに使用される特定のセキュリティ監査ツールでは、Cisco UmbrellaルートCAデジタル証明書に2048ビットのRSAキーがあり、2030年以降に有効期限が切れていることが報告される場合があります。ツールや組織のセキュリティポリシーによっては、キーサイズや有効期限に、修復が必要なリスクとしてフラグを付けることができます。この記事の情報を確認して、組織が監査ツールの推奨事項を受け入れる必要があるかどうかを判断してください。

NISTの推奨事項

時間の経過に伴うデジタル証明書キーの長さの推奨事項（2048ビットRSAキーの2030年の日付を含む）は、米国国立標準技術研究所(NIST)によって発行されました。 これらの推奨事項を記載した文書は、「SP 800-57 Part 1 Rev. 5: Recommendation for Key Management」です。

「表4、セキュリティ強度のタイムフレーム」（ページ59）は、112の対称キービットに相当するセキュリティ強度が、「レガシーの使用」に対して2030年以降は有効であることを示しています（RSA 2048ビットの非対称キーは、対称キー強度の約116ビットに相当します）。 Cisco UmbrellaルートCA証明書などの既存のルート証明書の使用はこのカテゴリに分類されるため、これは準拠した使用と見なされます。2030年以降に2048ビットキーで証明書を発行することは、この推奨事項に従いません。

その他の有名な公開認証局は、2048ビットのRSAキーを持つルート証明書と2030年以降の有効期限を引き続き使用しています。DigiCertのドキュメント「DigiCert Trusted Root Authority Certificates」を参照して、たとえばDigiCertによって発行されたグローバルルートCA証明書やAssured IDルートCA証明書などを確認します。

2030年より前に、Cisco UmbrellaはNISTの推奨事項に準拠した、より大きなキーサイズの新しいルート証明書を1つ以上発行できます。

追加情報

NISTの推奨事項が組織のニーズを満たしているかどうかは、組織が自由に判断できます。この問題についてさらに懸念がある場合は、シスコのTrusted Root Store & PKI Complianceプログラムを監督する専任のPKIチームが対応します。Cisco PKIチームからの追加情報（シスコが発行したすべての公開証明書、証明書のポリシーとプラクティスのステートメント、およびその他のドキュメントを含む）は、「Cisco PKI：ポリシー、証明書、およびドキュメント」で入手できます。その他の質問は、PKIチーム(ciscopki-public@external.cisco.com)に電子メールで送信できます。

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。