Résoudre les outils de sécurité Marquer l'autorité de certification racine Umbrella

Table des matières

Introduction

Ce document décrit pourquoi le certificat numérique d'autorité de certification racine Umbrella est marqué comme un risque par les outils d'audit de sécurité.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella Secure Web Gateway (SWG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Certains outils d'audit de sécurité utilisés pour analyser l'infrastructure Umbrella peuvent signaler que le certificat numérique CA racine Cisco Umbrella comporte une clé RSA 2048 bits et une expiration après 2030. En fonction de l'outil et de la stratégie de sécurité de l'entreprise, la taille de clé et/ou la date d'expiration peuvent être marquées comme un risque nécessitant une correction. Passez en revue les informations de cet article pour déterminer si votre organisation doit accepter les recommandations de l'outil d'audit.

Recommandations du NIST

Les recommandations relatives à la longueur de clé de certificat numérique dans le temps (y compris la date de 2030 pour les clés RSA de 2048 bits) ont été émises par le National Institutes of Standards (NIST) des États-Unis. Le document contenant ces recommandations est la disposition spéciale 800-57 Partie 1 Rév. 5 : Recommandation pour la gestion des clés.

Le « Tableau 4, Trames temporelles de sécurité » (page 59) indique qu'un équivalent de sécurité de 112 bits de clé symétrique est valide après 2030 pour une « utilisation traditionnelle » (les clés asymétriques RSA de 2 048 bits équivalent à environ 116 bits de sécurité symétrique). L'utilisation d'un certificat racine existant, tel que le certificat d'autorité de certification racine Cisco Umbrella, entre dans cette catégorie. Il s'agit donc d'une utilisation conforme. L'émission d'un certificat avec une clé de 2048 bits après 2030 ne serait pas conforme à la recommandation.

D'autres autorités de certification publiques bien connues continuent d'utiliser des certificats racines avec des clés RSA 2048 bits et des dates d'expiration après 2030. Consultez la documentation DigiCert : Certificats d'autorité racine de confiance DigiCert pour des exemples, tels que le certificat d'autorité de certification racine globale et le certificat d'autorité de certification racine d'ID assuré, émis par DigiCert.

Bien avant 2030, Cisco Umbrella peut émettre un ou plusieurs nouveaux certificats racine avec des clés de plus grande taille conformes aux recommandations du NIST.

Additional Information

Les organisations sont libres de décider si les recommandations du NIST répondent à leurs besoins. Si vous avez d'autres préoccupations concernant ce problème, Cisco dispose d'une équipe PKI dédiée qui supervise le programme Trusted Root Store & PKI Compliance de Cisco. Des informations supplémentaires de l'équipe ICP de Cisco (y compris tous les certificats publics émis par Cisco, les politiques de certification et les énoncés de pratiques, ainsi que d'autres documents) sont disponibles sur ICP de Cisco : Stratégies, certificats et documents. Des questions supplémentaires peuvent être envoyées par courriel à l'équipe de l'ICP à l'adresse ciscopki-public@external.cisco.com.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.