Resuelva las herramientas de seguridad marcando la CA raíz de Umbrella

Contenido

Introducción

Este documento describe por qué las herramientas de auditoría de seguridad marcan el certificado digital de la CA raíz de Umbrella como un riesgo.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella Secure Web Gateway (SWG).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Ciertas herramientas de auditoría de seguridad utilizadas para analizar la infraestructura de Umbrella pueden informar de que el certificado digital de CA raíz de Cisco Umbrella tiene una clave RSA de 2048 bits y una caducidad posterior a 2030. En función de la herramienta y de la política de seguridad de la organización, el tamaño de la clave o la fecha de caducidad se pueden marcar como un riesgo que puede requerir una solución. Revise la información de este artículo para determinar si su organización debe aceptar las recomendaciones de la herramienta de auditoría.

Recomendaciones del NIST

Las recomendaciones para la longitud de la clave del certificado digital a lo largo del tiempo (incluida la fecha de 2030 para las claves RSA de 2048 bits) fueron emitidas por los Institutos Nacionales de Estándares (NIST) de EE. UU. El documento que contiene estas recomendaciones es SP 800-57 Parte 1 Rev. 5: Recomendación para la administración de claves.

"Tabla 4, Plazos de seguridad" (página 59) indica que un equivalente de 112 bits de clave simétrica de seguridad es válido después de 2030 para "Uso heredado" (las claves asimétricas de RSA de 2048 bits equivalen aproximadamente a 116 bits de clave simétrica). El uso de un certificado raíz existente como el certificado de CA raíz de Cisco Umbrella pertenece a esta categoría, por lo que se considera un uso compatible. Emitir un certificado con una clave de 2048 bits después de 2030 no cumpliría con la recomendación.

Otras autoridades de certificación públicas conocidas continúan utilizando certificados raíz con claves RSA de 2048 bits y fechas de vencimiento posteriores a 2030. Revise la documentación de DigiCert: Certificados de autoridad raíz de confianza de DigiCert para ejemplos, como el certificado de CA raíz global y el certificado de CA raíz de ID garantizada, emitido por DigiCert.

Mucho antes de 2030, Cisco Umbrella puede emitir uno o más certificados raíz nuevos con tamaños de clave más grandes que cumplan con las recomendaciones del NIST.

Additional Information

Las organizaciones son libres de decidir si las recomendaciones del NIST satisfacen sus necesidades. Si le preocupa más este problema, Cisco cuenta con un equipo PKI dedicado que supervisa el programa Trusted Root Store & PKI Compliance. Puede encontrar información adicional del equipo de Cisco PKI (incluidos todos los certificados públicos emitidos por Cisco, las políticas de certificados y las declaraciones de prácticas, así como otra documentación) en Cisco PKI: Directivas, certificados y documentos. Se pueden enviar preguntas adicionales por correo electrónico al equipo de PKI en ciscopki-public@external.cisco.com.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).