Resolver Ferramentas de Segurança Sinalizando a CA Raiz do Guarda-Chuva

Contents

Introdução

Este documento descreve por que o certificado digital da CA raiz do Umbrella é sinalizado como um risco pelas ferramentas de auditoria de segurança.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella Secure Web Gateway (SWG).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Determinadas ferramentas de auditoria de segurança usadas para verificar a infraestrutura do Umbrella podem relatar que o certificado digital da CA raiz do Cisco Umbrella tem uma chave RSA de 2048 bits e um vencimento após 2030. Dependendo da ferramenta e da política de segurança da organização, o tamanho da chave e/ou a data de expiração pode ser sinalizada como um risco que pode exigir correção. Revise as informações neste artigo para determinar se sua organização precisa aceitar as recomendações da ferramenta de auditoria.

Recomendações NIST

As recomendações para o comprimento da chave de certificado digital ao longo do tempo (incluindo a data de 2030 para chaves RSA de 2048 bits) foram emitidas pelo National Institutes of Standards (NIST) dos EUA. O documento contendo estas recomendações é SP 800-57 Parte 1 Rev. 5: Recomendação para Gerenciamento de Chaves.

A "Tabela 4, Tempos limite de segurança" (página 59) indica que um Security Strength equivalente a 112 bits de chave simétrica é válido após 2030 para "Uso herdado" (chaves assimétricas RSA de 2048 bits são equivalentes a aproximadamente 116 bits de força de chave simétrica). O uso de um certificado raiz existente, como o certificado da CA raiz do Cisco Umbrella, se enquadra nessa categoria, então isso seria considerado um uso compatível. A emissão de um certificado com uma chave de 2048 bits após 2030 não cumpriria a recomendação.

Outras autoridades públicas de certificação conhecidas continuam a usar certificados raiz com chaves RSA de 2048 bits e datas de expiração após 2030. Revise a documentação do DigiCert: Certificados de autoridade de raiz confiável DigiCert para obter exemplos, como o certificado de autoridade de certificação raiz global e o certificado de autoridade de certificação raiz de ID garantida, emitidos pela DigiCert.

Muito antes de 2030, o Cisco Umbrella pode emitir um ou mais novos certificados raiz com tamanhos de chave maiores que estejam em conformidade com as recomendações do NIST.

Informações adicionais

As organizações são livres para decidir se as recomendações do NIST atendem às suas necessidades. Se você tiver mais preocupações sobre esse problema, a Cisco tem uma equipe de PKI dedicada que supervisiona o programa de conformidade com PKI e armazenamento raiz confiável da Cisco. Informações adicionais da equipe de PKI da Cisco (incluindo todos os certificados públicos emitidos pela Cisco, políticas de certificado e declarações práticas e outra documentação) estão disponíveis no PKI da Cisco: Políticas, certificados e documentos. Perguntas adicionais podem ser enviadas por e-mail para a equipe de PKI em ciscopki-public@external.cisco.com.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.