Solve Security Tools Flagging the Umbrella Root CA

Contents

Introduction

This document describes why the Umbrella Root CA digital certificate is flagged as a risk by security auditing tools.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

Overview

Certain security auditing tools used to scan Umbrella infrastructure can report that the Cisco Umbrella Root CA digital certificate has a 2048-bit RSA key and an expiration after 2030. Depending on the tool and the organization's security policy, the key size and/or expiration date can be flagged as a risk which can require remediation. Review the information in this article to determine whether your organization needs to accept the auditing tool's recommendations.

NIST Recommendations

The recommendations for digital certificate key length over time (including the 2030 date for 2048-bit RSA keys) were issued by the US National Institutes of Standards (NIST). The document containing these recommendations is SP 800-57 Part 1 Rev. 5: Recommendation for Key Management.

"Table 4, Security strength time frames" (page 59) indicates that a Security Strength equivalent of 112 symmetric key bits is valid after 2030 for "Legacy use" (RSA 2048-bit asymmetric keys are equivalent to approximately 116 bits of symmetric key strength). The use of an existing root certificate such as the Cisco Umbrella Root CA certificate falls into this category, so this would be considered compliant use. Issuing a certificate with a 2048-bit key after 2030 would not comply with the recommendation.

Other well-known public certificate authorities continue to use root certificates with 2048-bit RSA keys and expiration dates after 2030. Review DigiCert documentation: DigiCert Trusted Root Authority Certificates for examples, such as the Global Root CA certificate and the Assured ID Root CA certificate, issued by DigiCert.

Well before 2030, Cisco Umbrella can issue one or more new root certificates with larger key sizes that comply with NIST recommendations.

Additional Information

Organizations are free to decide whether the NIST recommendations meet their needs. If you have further concerns about this issue, Cisco has a dedicated PKI team which oversees Cisco's Trusted Root Store & PKI Compliance program. Additional information from the Cisco PKI team (including all Cisco-issued public certificates, certificate policies and practice statements, and other documentation) is available at Cisco PKI: Policies, Certificates, and Documents. Additional questions can be emailed to the PKI team at ciscopki-public@external.cisco.com.