

Umbrella Root CA 플래그 지정 보안 툴 해결

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [개요](#)
 - [NIST 권장 사항](#)
 - [추가 정보](#)
-

소개

이 문서에서는 Umbrella Root CA 디지털 인증서가 보안 감사 툴에 의해 위협으로 플래그가 지정된 이유를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella SWG(Secure Web Gateway)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella 인프라를 스캔하는 데 사용되는 특정 보안 감사 도구는 Cisco Umbrella Root CA 디지털 인증서에 2048비트 RSA 키가 있으며 2030년 이후에 만료됨을 보고할 수 있습니다. 툴 및 조직의 보안 정책에 따라 키 크기 및/또는 만료 날짜가 위협(교정이 필요할 수 있음)으로 표시될 수 있습니다. 조직에서 감사 도구의 권장 사항을 수락해야 하는지 여부를 확인하려면 이 문서의 정보를 검토하십시오.

NIST 권장 사항

시간에 따른 디지털 인증서 키 길이(2048비트 RSA 키의 2030년 날짜 포함)에 대한 권장 사항은 US NIST(National Institute of Standards)에서 발표했습니다. 이러한 권장 사항이 포함된 문서는 SP

800-57 Part 1 수정 버전 5입니다. 키 관리 권장 사항

"표 4, 보안 강도 시간 프레임"(59페이지)은 "레거시 사용"에 대해 2030년 이후에 112개의 대칭 키 비트에 해당하는 보안 강도가 유효함을 나타냅니다(RSA 2048비트 비대칭 키는 대칭 키 강도 약 116비트에 해당합니다). Cisco Umbrella Root CA 인증서와 같은 기존 루트 인증서를 사용하는 경우 이 카테고리에 속하므로 이는 규정 준수 용도로 간주됩니다. 2030년 이후에 2048비트 키로 인증서를 발급하는 것은 그 권고를 따르지 않을 것이다.

다른 잘 알려진 공개 인증 기관에서는 2048비트 RSA 키와 2030년 이후의 만료 날짜가 포함된 루트 인증서를 계속 사용합니다. DigiCert 문서를 검토합니다. 예를 들어 DigiCert에서 발급하는 전역 루트 CA 인증서 및 Assured ID 루트 CA 인증서와 같은 DigiCert의 신뢰할 수 있는 루트 인증 기관 인증서

2030년 이전에는 Cisco Umbrella가 NIST 권장 사항을 준수하는 더 큰 키 크기를 가진 하나 이상의 새 루트 인증서를 발급할 수 있습니다.

추가 정보

조직은 NIST 권장 사항이 요구 사항을 충족하는지 자유롭게 결정할 수 있습니다. 이 문제에 대한 추가 우려가 있는 경우 Cisco에는 Cisco의 신뢰할 수 있는 루트 저장소 및 PKI 규정 준수 프로그램을 감독하는 전담 PKI 팀이 있습니다. Cisco PKI 팀의 추가 정보(모든 Cisco 발급 공용 인증서, 인증서 정책 및 실무 설명, 기타 문서 포함)는 [Cisco PKI](#)에서 확인할 수 있습니다. [정책, 인증서 및 문서](#). 추가 질문은 PKI 팀(ciscopki-public@external.cisco.com)으로 이메일을 보내 주십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.