

解决标记Umbrella Root CA的安全工具

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[概述](#)

[NIST建议](#)

[Additional Information](#)

简介

本文档说明安全审计工具将Umbrella Root CA数字证书标记为风险的原因。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella安全Web网关(SWG)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

某些用于扫描Umbrella基础设施的安全审核工具可以报告Cisco Umbrella Root CA数字证书具有2048位RSA密钥，并且将在2030年之后过期。根据工具和组织的安全策略，可以将密钥大小和/或到期日期标记为可能需要补救的风险。查看本文中的信息，以确定您的组织是否需要接受审计工具的建议。

NIST建议

数字证书密钥长度随时间变化的建议（包括2030日期的2048位RSA密钥）由美国国家标准研究院(NIST)发布。包含这些建议的文档是SP 800-57第1部分修订版5:密钥管理建议。

“表4，安全强度时间帧”（第59页）表明，相当于112个对称密钥位的安全强度在2030年之后对于“传统使用”是有效的（RSA 2048位非对称密钥相当于大约116位的对称密钥强度）。现有根证书（例

如Cisco Umbrella根CA证书)的使用属于此类别，因此这被视为合规使用。在2030年之后签发带有2048位密钥的证书不符合建议。

其他著名的公共证书颁发机构继续使用具有2048位RSA密钥的根证书和2030年后的到期日期。查看DigiCert文档：例如，DigiCert颁发的全局根CA证书和保证ID根CA证书等DigiCert受信任根授权证书。

在2030年之前，Cisco Umbrella可以颁发一个或多个新的根证书，其密钥大小更大，符合NIST建议。

Additional Information

组织可以自由决定NIST建议是否满足其需求。如果您对此问题有进一步的担忧，思科有一个专门的PKI团队，负责监督思科的Trusted Root Store & PKI Compliance计划。[Cisco](#) PKI提供了来自Cisco PKI团队的其他信息（包括所有思科颁发的公共证书、证书策略和实践声明以及其他文档）：[策略、证书和文档](#)。如有其他问题，可通过电邮发送至PKI团队：ciscopki-public@external.cisco.com。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。