更新DNS Umbrella证书于2024年10月生效

目录

简介

本文档介绍如何解决SD-WAN路由器使用过期证书而非新证书的DNS Umbrella问题。

背景信息

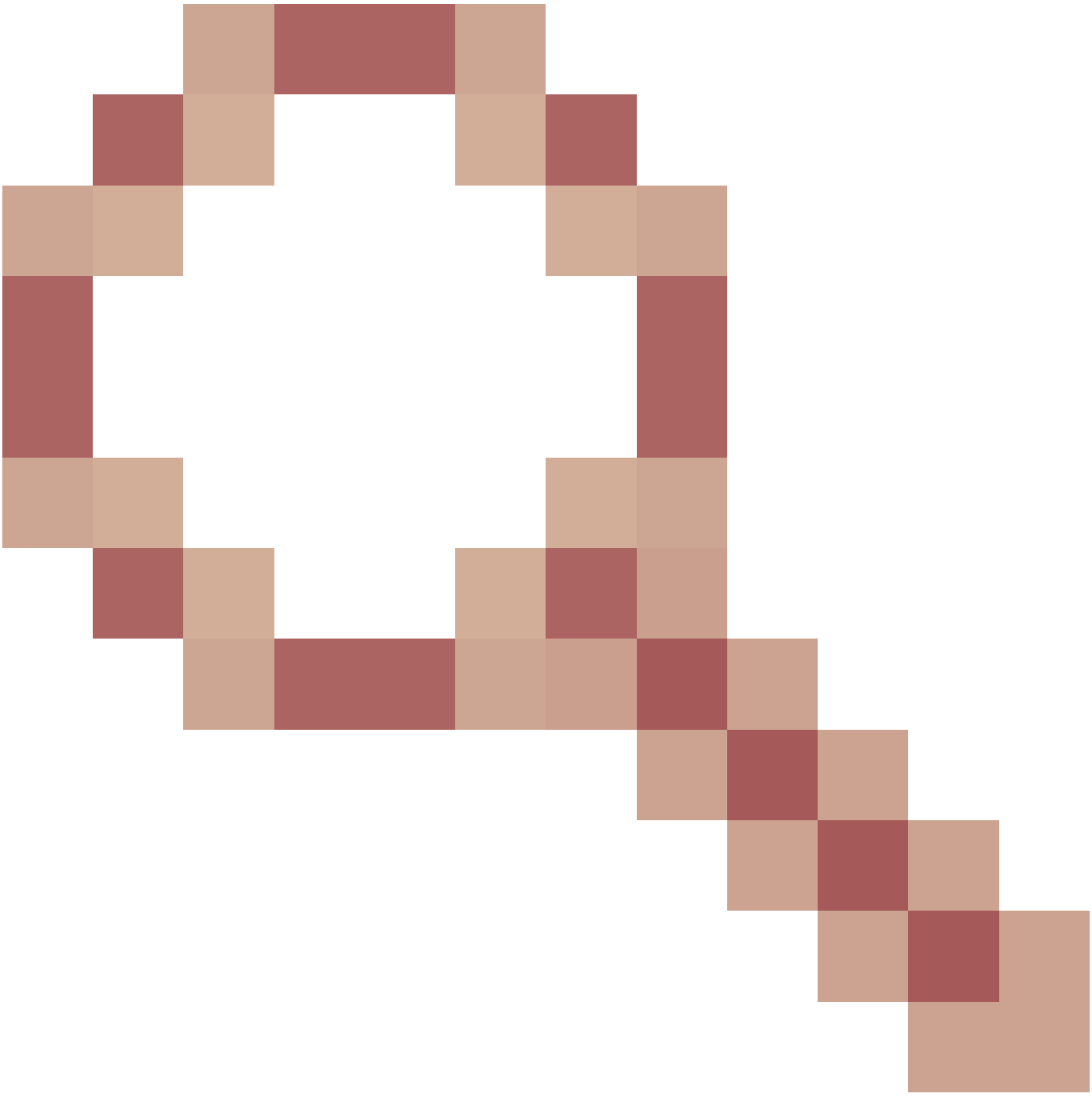
Cisco Catalyst SD-WAN路由器用于在Cisco Umbrella DNS中使用API密钥/密钥身份验证方法进行注册的数字证书已于2024年9月30日到期。证书过期的Cisco SD-WAN路由器将无法注册到Cisco Umbrella DNS服务。此问题不适用于Umbrella DNS注册的基于令牌的身份验证。

有关详细信息，请参阅Cisco Umbrella DNS证书于2024年9月30日到期，位置通知FN74166。

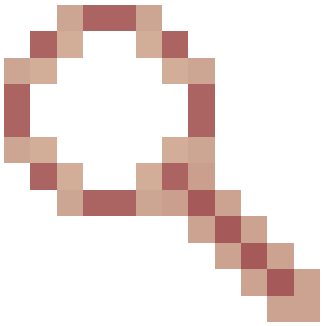
具有已过期umbrella根CA证书的受影响SD-WAN设备无法与Cisco Umbrella DNS建立安全连接以进行设备注册。 由于设备未向Umbrella DNS服务注册，因此SD-WAN边缘不会将最终用户DNS请求重定向到Umbrella域服务器以执行DNS安全策略。来自SD-WAN边缘后方最终用户的DNS请求不会被丢弃，并由最终用户设备上配置的DNS域服务器提供服务。

缺陷信息

证书已作为Cisco Bug ID CSCwi43360（仅限注册用户）的一部分进行更新



：Umbrella云的DNS安全注册证书将于2024年9月到期。（在17.9.6、17.12.4、17.15.1a中修复）



即使证书已更新，SSL握手也无法建立，这作为Cisco Bug ID CSCwm73365
： SSL握手失败，尽管umbrella_root_ca.ca和设备上存在最新的证书。（已在17.6.8a中修正）

已发布固定版本

CCO版本

版本	17.6.8安

补救表

版本	思科建议的补救步骤
17.3.x/17.4.x/17.5.x	请执行1中的步骤。在控制器模式下运行Cisco IOS XE软件版本17.5.x或更早版本的Cisco设备
17.6.1-17.6.7、17.7.x、17.8.x	请按照第2部分中的步骤进行操作。在控制器模式下运行Cisco IOS XE软件版本17.6.x到17.8.x的Cisco设备
17.6.8安	Umbrella DNS证书到期问题在此版本中已修复。
17.9.1 – 17.9.4、17.10.x、17.11.x、17.12.1-17.12.2、17.13.x、17.14.x、17.15.1a	请使用Umbrella DNS证书脚本将证书自动复制到边缘设备。有关运行脚本的步骤，请参阅GIT上的自述文件。
17.9.5安	按照第3部分中的步骤进行操作
17.9.6	执行第4部分中的步骤
17.12.3安	请按照第5节中的步骤操作
17.12.4	执行第6部分中的步骤

1. 在控制器模式下运行Cisco IOS XE软件版本17.5.x或更早版本的Cisco设备

使用补救选项安装新的Umbrella RootCA证书。

1. 自动：

1. 对于SD-WAN Manager 20.9.1或更高版本，请使用Umbrella DNS证书脚本从vManage自动将证书复制到边缘设备。
2. Umbrela DNS证书脚本
3. 有关使用该脚本的详细步骤，请参阅GIT上的自述文件。
4. 将RootCA证书复制到设备后，重新加载路由器以完成安装过程。

2. 手动：

1. 从New Umbrella Certificate网站下载新的未过期证书，并将其放置在SD-WAN重叠中能够访问受影响路由器的设备上。
2. 输入Linux scp命令或类似机制，执行从下载设备到每个受影响路由器的安全文件复制。

例如：

scp ./isrgrootx1.pem <用户名>@<边缘IP>：trustidrootx3_ca.ca

用管理员用户替换<Username>，用受影响路由器的IP地址替换<EdgeIP>。

c.将RootCA证书复制到设备后，重新加载路由器以完成安装过程。

2. 在控制器模式下运行Cisco IOS XE软件版本17.6.x到17.8.x的Cisco设备

使用补救选项安装新的Umbrella RootCA证书。

1. 自动：

1. 对于SD-WAN Manager 20.9.1或更高版本，请使用Umbrella DNS证书脚本从vManage自动将证书复制到边缘设备。
2. Umbrella DNS证书脚本
3. 有关使用该脚本的详细步骤，请参阅GIT上的自述文件。
4. 将RootCA证书复制到设备后，重新加载路由器以完成安装过程。

2. 手册：

1. 从New Umbrella Certificate网站下载新的未过期证书，并将其放置在SD-WAN重叠中能够访问受影响路由器的设备上。
2. 输入Linux scp命令或类似机制，以便将安全文件从下载设备复制到每个受影响的路由器上。

例如：

scp ./isrgrootx1.pem admin@<边缘IP>：trustidrootx3_ca_092024.ca

用受影响路由器的IP地址替换<EdgeIP>。

c.将RootCA证书复制到设备后，重新加载路由器以完成安装过程

3. 在控制器模式下运行Cisco IOS XE软件版本17.9.5a的Cisco设备

使用补救选项安装新的Umbrella RootCA证书（如本节所述），对于大多数平台而言，有一个热SMU随修补程序一起提供。您还可以选择运行上述脚本以安装新的Umbrella RootCA证书。

1. HOT SMU适用于这些平台-“无中断/建议的SMU，SSL握手失败，尽管umbrella_root_ca.ca和最新证书存在于设备上”：

4431 集成多业务路由器
4451-X集成多业务路由器

ASR 1001-X路由器
虚拟路由器
4331 集成多业务路由器
4221 集成多业务路由器
4351 集成多业务路由器
Catalyst 8500L Edge平台
ASR 1001-HX路由器
4321 集成多业务路由器

Catalyst 8500边缘平台

4461 集成多业务路由器

2. 或者，运行Umbrella DNS Cert Script脚本，参阅GIT上的自述文件，了解使用该脚本的详细步骤。

仅脚本选项：
ASR1002-X路由器

Catalyst 8300边缘平台

运行Cisco IOS XE SD-WAN的ISR 1000系列

4. 在控制器模式下运行Cisco IOS XE软件版本17.9.6的Cisco设备

1. HOT SMU适用于这些平台- “无中断/建议的SMU，SSL握手失败，尽管umbrella_root_ca.ca和最新证书存在于设备上”：

4221 集成多业务路由器
4321 集成多业务路由器
4451-X集成多业务路由器
Catalyst 8500边缘平台
4431 集成多业务路由器
虚拟路由器
4461 集成多业务路由器
4331 集成多业务路由器
4351 集成多业务路由器
ASR 1001-HX路由器
ASR 1001-X路由器
Catalyst 8500L Edge平台

3. 或者，运行Umbrella DNS Cert Script脚本，参阅GIT上的自述文件，了解使用该脚本的详细步骤。

仅脚本选项：

ASR1002-X路由器

Catalyst 8300边缘平台

运行Cisco IOS XE SD-WAN的ISR 1000系列

5. 控制器模式下的Cisco IOS XE软件版本17.12.3a的Cisco设备

1. HOT SMU适用于这些平台- “无中断/建议的SMU，SSL握手失败，尽管umbrella_root_ca.ca和最新证书存在于设备上”：

4221 集成多业务路由器
Catalyst 8300边缘平台
4331 集成多业务路由器
4461 集成多业务路由器
1100 集成多业务路由器
4351 集成多业务路由器
4321 集成多业务路由器
4431 集成多业务路由器
虚拟路由器
4451-X集成多业务路由器

2. 除SMU之外，运行脚本Umbrella DNS Cert Script

有关使用该脚本的详细步骤，请参阅GIT上的自述文件。

6. 在控制器模式下运行Cisco IOS XE软件版本17.12.4的Cisco设备

1. HOT SMU适用于这些平台- “无中断/建议的SMU，SSL握手失败，尽管umbrella_root_ca.ca和最新证书存在于设备上”：

Catalyst 8500边缘平台
ASR 1001-HX路由器
4331 集成多业务路由器
4321 集成多业务路由器
4221 集成多业务路由器
虚拟路由器
4351 集成多业务路由器
4451-X集成多业务路由器
4461 集成多业务路由器
Catalyst 8300边缘平台
ASR 1002-HX路由器
4431 集成多业务路由器

1100 集成多业务路由器

Catalyst 8500L Edge平台

2. SMU的备用方法是运行脚本Umbrella DNS Cert Script。有关使用该脚本的详细步骤，请参阅GIT上的自述文件。

⚠ 警告：只要设备未重新启动或未进行新注册，来自设备的Umbrella DNS注册将继续运行。

⚠ 注意：如果删除并重新应用Umbrella配置，则会触发Umbrella DNS的重新注册。只要不遵循此过程，UMBRELLA DNS就会正常工作。

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）。