在Umbrella集成访问期间排除证书过期错误

目录

简介

本文档介绍如何对Umbrella集成访问s-platform.api.opendns.com或fireeye.vendor.api.opendns.com时的证书过期错误进行故障排除。

问题

使用某些第三方客户端的Umbrella集成可能会失败，因为在s-platform.api.opendns.com and fireeye.vendor.api.opendns.com上验证Umbrella API服务器的数字证书时出错。错误文本或代码因集成中使用的客户端程序而异，但通常表示存在过期的证书。

原因

此问题不是由当前有效的服务器证书引起的。相反，此问题是由客户端使用的过期证书信任存储引起的。

为s-platform.api.opendns.com和fireeye.vendor.api.opendns.com提供服务的Web服务器使用由证书颁发机构Let's Encrypt的中间证书R3颁发的数字证书（该数字证书经过数字签名）。R3使用公钥进行签名，该公钥可在当前 SRG Root X1 root certificate from Let's Encrypt和SRG Root X1的旧交叉签名版本。因此，存在两个验证路径：一个终止于当前SRG根X1，另一个终止于交叉签名版本(由证书颁发机构IdenTrust颁发的DST根CA X3证书)的颁发者。

Let's Encrypt中提供了颁发过程图。此外，Qualys SSL Labs工具可用于查看两个“认证路径”，以及相应的证书和证书详细信息（如到期日期）。

根证书保存在客户端系统上的一个或多个证书信任库中。2021年9月30日，DST根CA X3证书到期。自此日期以来，在其信任存储中具有DST根CA X3证书，但没有较新的RG根X1根证书的客户端，由于证书错误，无法连接到s-platform.api.opendns.com或fireeye.vendor.api.opendns.com。 错误消息或代码可能指示过期的证书作为错误的原因。过期的证书是客户端信任存储中的DST根CA X3证书，而不是API服务器(s-platform.api.opendns.com和fireeye.vendor.api.opendns.com)的服务器证书。

分辨率

要解决此问题，请更新客户端的信任存储以包含新的SRG根X1证书，该证书可以从Let's Encrypt网站下载。（此页面还提供用于测试客户端的网站。）请参阅客户端或操作系统的文档，获取有关查看和更新客户端信任库的说明。如果正式更新包或自动更新机制可用，则这通常比手动更新信任库更可取。

如果使用新的SRG根X1证书手动更新信任存储，我们还建议删除过期的DST根CA X3证书，以防客户端的验证路径生成代码出现问题。客户端或操作系统的提供商对信任存储的正式更新可以添加SRG根X1并删除DST根CA X3证书。

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）。