Splunk客户端日志上传的安全访问证书验证错误

目录

问题

运行Splunk客户端的Windows客户端无法向Splunk云上传日志，因为当流量被Cisco安全访问解密时，出现了证书验证错误。超过5000个Windows日志源无法向Splunk云发送数据，从而影响日志接收。在Splunk客户端日志中观察到的特定错误为：

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

流向目标*.splunkcloud.com的流量通过防火墙流动，但应用级证书验证失败。浏览到启用SSL解密的站点的网络继续正常运行。

环境

- 启用SSL/TLS解密的思科安全访问
- 安装了Splunk Universal Forwarder的Windows客户端
- Splunk云目标：*.splunkcloud.com
- 受影响的Windows日志源超过5000个
- Splunk客户端使用其自己的证书存储区，而不是Microsoft系统证书存储区

分辨率

通过在思科安全访问中为Splunk云流量实施解密旁路策略解决了此问题。

已经采取了若干步骤。

步骤 1：识别问题

在WebEx会议期间，确认并再现了此行为。测试表明，当客户端禁用安全访问解密或客户端禁用SWG服务时，Splunk日志上传成功。这确认了SSL/TLS解密过程导致证书验证失败。

步骤 2：创建目标列表

创建了一个包含Splunk云FQDN和IP地址的目标列表，以明确针对发往Splunk云服务的流量。

步骤 3：实施解密旁路策略

实施思科安全访问策略以禁用匹配Splunk云目标列表的流量的SSL/TLS解密。此旁路策略允许Splunk客户端建立到Splunk云的直接加密连接，而无需安全访问拦截证书。

步骤 4：验证

实施解密旁路策略后，验证确认：

- Splunk客户端能够成功上传日志
- Splunk云中报告客户端的总数显着增加
- 未发现其他证书验证错误

案例严重性从1减到3，并置于监控状态以观察持续成功的日志摄取。

原因

根本原因是Splunk客户端使用其自己的证书存储区，并且不信任在SSL/TLS解密过程中呈现的Cisco安全访问主SubCA证书。当思科安全访问拦截和解密到Splunk云的SSL流量时，它会使用其自己的证书颁发机构重新加密该流量。Splunk客户端证书验证进程拒绝此证书，因为它无法向自身证书存储中的受信任根证书颁发机构验证证书链。

特定X.509验证错误“无法获取本地颁发者证书”（错误代码20）表示证书验证进程无法在客户端受信任证书存储中找到颁发证书颁发机构，从而导致连接失败。

相关内容

- 思科技术支持和下载

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）。