

由于Codex应用DNS风暴，安全客户端Umbrella模块变为非活动状态

目录

问题

MacOS上的多个用户会遇到思科安全客户端Umbrella漫游模块间歇性地转换到非活动（失效开放）状态。在这些期间，DNS请求（包括终端发起的nslookup命令）无法到达网络层，从而影响用户解析域和访问基于互联网的资源的能力。

问题在Umbrella日志中反复出现探测失败，显示如下消息：

```
Transparent probe failed
Encrypted probe failed
Switching to basic probe
DNS probe failed by timeout - going open
```

分析显示，当Umbrella处于非活动状态时，Acsock驱动程序在同一故障窗口内崩溃。在用户主动使用Codex和AI Assistant应用时，最常发现此问题，在向CODEX发送命令后，大量连接会立即尝试连接到chatgpt.com。

环境

- 思科安全客户端版本5.1.13、5.1.16、5.1.17
- macOS（观察到多个版本）
- Umbrella漫游模块已启用
- 启用ZTNA/安全互联网接入(SIA)模块
- Codex应用程序正在使用

- 使用各种网络 (家庭、办公室、不同ISP) 的用户

分辨率

通过实施域旁路配置来防止DNS请求重复，问题得以解决。对以下各节中介绍的方法进行了验证。

主分辨率：域绕行

- 步骤 1：将chatgpt.com添加到Cisco安全访问配置的旁路列表中。这可防止安全客户端复制Codex应用生成的DNS请求，从而消除导致驱动程序不稳定的DNS风暴。
- 步骤 2：检验旁路配置。测试Codex功能，确认旁路就绪后，问题不再重现。

备选解决方案：Codex配置解决方法

应用GitHub问题中引用的代码配置更改，以减少应用程序生成的DNS请求量。

<https://github.com/openai/codex/issues/21218>

使用的高级故障排除步骤

执行这些诊断步骤以确定根本原因。

1. — 启用详细附件日志记录：

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -sdf 0x830801F2
```

2. — 重现问题，并在出现故障后立即收集DART套件。

3. — 禁用详细日志记录：

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4. — 启用SWG的最大调试日志记录。创建包含内容的SWGConfigOverride.json文件：

```
{"logLevel": "1"}
```

保存到/opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json。

5. — 启用DNS的RSM跟踪日志。创建包含内容的force_log_level.plist文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

保存到/opt/cisco/secureclient/umbrella/data。

原因

核心问题与Codex应用行为有关，Codex应用行为会生成大量的DNS请求。如果未绕过chatgpt.com,Cisco Secure Client会有效复制这些请求，从而产生一个DNS风暴，导致CPU使用率高和缓存内核驱动程序不稳定。

出现此问题的原因如下：

- Codex在操作过程中生成大量到chatgpt.com的DNS查询。
- 如果没有旁路配置，安全客户端将拦截并复制这些请求。
- 大量重复的DNS请求会导致缓存驱动程序崩溃。
- 驱动程序不稳定会导致Umbrella探测器故障和转换到失效开放状态。

当绕过chatgpt.com或应用Codex解决方法时，不会发生这种重复，问题不再重现。此问题同时影响仅适用于Umbrella的配置和ZTNA SIA配置，表明问题出在流量处理机制而非特定模块内。

相关内容

- [安全访问漫游模块故障排除](#)
- [排除故障并收集基本信息](#)
- [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）。

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）。