

Secure Client Umbrella-Modul wird aufgrund von DNS-Sturm der Codex-Anwendung inaktiv

Inhalt

Problem

Das Cisco Secure Client Umbrella Roaming-Modul wird unter MacOS von mehreren Benutzern mit Unterbrechungen in einen inaktiven (Fail-Open) Zustand versetzt. Während dieser Zeiträume erreichen DNS-Anfragen, einschließlich Terminal-initiiertem nslookup-Befehl, die Netzwerkschicht nicht, was sich auf die Fähigkeit der Benutzer auswirkt, Domänen aufzulösen und auf internetbasierte Ressourcen zuzugreifen.

Das Problem manifestiert sich mit wiederholten Testfehlern in Umbrella-Protokollen, die Meldungen wie die folgenden enthalten:

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

Die Analyse hat ergeben, dass der Accock-Treiber während desselben Fehlerfensters abstürzt, wenn Umbrella inaktiv wird. Das Problem wird am häufigsten beobachtet, wenn Benutzer aktiv Codex- und AI Assistant-Anwendungen verwenden und sofort nach der Übermittlung von Befehlen an CODEX zahlreiche Verbindungsversuche an chatgpt.com unternommen werden.

Umwelt

- Cisco Secure Client, Versionen 5.1.13, 5.1.16, 5.1.17
- macOS (mehrere Versionen beobachtet)
- Umbrella-Roaming-Modul aktiviert

- ZTNA-/SIA-Modul aktiviert
- Codex-Anwendung in Gebrauch
- Benutzer, die von verschiedenen Netzwerken (zu Hause, im Büro, von verschiedenen ISPs) aus arbeiten

Auflösung

Das Problem wurde durch die Implementierung von Domänenumgehungskonfigurationen behoben, um die Duplizierung von DNS-Anforderungen zu verhindern. Die in den nächsten Abschnitten beschriebenen Ansätze wurden validiert.

Primäre Auflösung: Domain-Umgehung

- Schritt 1: Fügen Sie chatgpt.com zur Umgehungsliste in der Cisco Secure Access-Konfiguration hinzu. Dadurch wird verhindert, dass der Secure Client von der Codex-Anwendung generierte DNS-Anfragen dupliziert und der DNS-Sturm, der die Instabilität des Treibers verursacht, beseitigt.
- Phase 2: Überprüfen Sie die Bypass-Konfiguration. Testen Sie die Codex-Funktion, um sicherzustellen, dass das Problem nicht mehr reproduziert wird, wenn der Bypass vorhanden ist.

Alternative Auflösung: Problemumgehung bei der Codex-Konfiguration

Wenden Sie die Codex-Konfigurationsänderungen an, auf die im GitHub-Problem verwiesen wird, um die Anzahl der von der Anwendung generierten DNS-Anfragen zu reduzieren.

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

Verwendete erweiterte Schritte zur Fehlerbehebung

Diese Diagnoseschritte wurden durchgeführt, um die Ursache zu identifizieren.

1.- Aktivieren Sie ausführliche Systemprotokollierung:

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

2.- Reproduzieren Sie das Problem, und sammeln Sie das DART-Paket direkt nach dem Fehler.

3.- Deaktivieren der Protokollierung:

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

4.- Aktivieren Sie die maximale Debug-Protokollierung für SWG. Erstellen Sie die Datei "SWGConfigOverride.json" mit folgendem Inhalt:

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

Speichern Sie die Datei unter /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- RSM-Ablaufverfolgungsprotokolle für DNS aktivieren. Erstellen Sie die Datei force_log_level.plist mit Inhalt:

```
<?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>
```

Speichern Sie unter /opt/cisco/secureclient/umbrella/data.

Ursache

Das Kernproblem ist das Verhalten der Codex-Anwendung, die sehr viele DNS-Anfragen

generiert. Wenn chatgpt.com nicht umgangen wird, werden diese Anforderungen vom Cisco Secure Client effektiv dupliziert, wodurch ein DNS-Sturm entsteht, der zu einer hohen CPU-Auslastung und einer Instabilität des Core-Kerneltreibers führt.

Das Problem tritt aus folgenden Gründen auf:

- Codex generiert während des Betriebs zahlreiche DNS-Abfragen an chatgpt.com.
- Ohne Umgehungskonfiguration fängt Secure Client diese Anforderungen ab und dupliziert sie.
- Die große Anzahl an duplizierten DNS-Anfragen führt zum Absturz des Systemtreibers.
- Die Instabilität des Treibers führt zu Umbrella-Testfehlern und dem Übergang in den Fail-Open-Status.

Wenn chatgpt.com umgangen wird oder die Codex-Problemumgehung angewendet wird, tritt diese Duplizierung nicht auf, und das Problem wird nicht mehr reproduziert. Das Problem betrifft sowohl Umbrella-only- als auch ZTNA-SIA-Konfigurationen, was darauf hinweist, dass das Problem nicht in einem bestimmten Modul, sondern im Datenverkehrsverarbeitungsmechanismus liegt.

Verwandte Inhalte

- [Fehlerbehebung für Secure Access Roaming-Modul](#)
- [Fehlerbehebung und Erfassung grundlegender Informationen](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.