

Secure Client Umbrella Module wordt inactief vanwege DNS-storm in Codex-toepassing

Inhoud

uitgifte

Meerdere gebruikers op macOS ervaren de Cisco Secure Client Umbrella-roamingmodule die met tussenpozen overgaat naar een inactieve (failopen) status. Tijdens deze perioden bereiken DNS-verzoeken, inclusief nslookup-opdrachten die door terminals zijn geïnitieerd, de netwerklaag niet, wat van invloed is op de mogelijkheid van gebruikers om domeinen op te lossen en toegang te krijgen tot internetbronnen.

Het probleem manifesteert zich met herhaalde probe-fouten in Umbrella-logboeken, met berichten zoals:

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

Analyse toonde aan dat de stuurprogramma crasht tijdens hetzelfde uitvalvenster wanneer Umbrella inactief wordt. Het probleem wordt het vaakst waargenomen terwijl gebruikers actief Codex- en AI Assistant-toepassingen gebruiken, met een groot aantal verbindingspogingen naar chatgpt.com onmiddellijk na opdrachten die naar CODEX zijn verzonden.

milieu

- Cisco Secure Client versies 5.1.13, 5.1.16, 5.1.17
- macOS (meerdere versies waargenomen)
- Umbrella Roaming Module ingeschakeld

- ZTNA/Secure Internet Access (SIA)-module ingeschakeld
- Codex-toepassing in gebruik
- Gebruikers die werken vanuit verschillende netwerken (thuis, op kantoor, verschillende ISP's)

resolutie

Het probleem is opgelost door het implementeren van domeinbypass-configuraties om duplicatie van DNS-aanvragen te voorkomen. De in de volgende paragrafen beschreven benaderingen werden gevalideerd.

Primaire resolutie: domeinbypass

- Stap 1: Voeg chatgpt.com toe aan de bypass-lijst in de Cisco Secure Access-configuratie. Dit voorkomt dat de beveiligde client DNS-verzoeken die door de Codex-toepassing zijn gegenereerd, dupliceert, waardoor de DNS-storm die stuurprogramma-instabiliteit veroorzaakt, wordt geëlimineerd.
- Stap 2: Controleer de bypass-configuratie. Test de Codex-functionaliteit om te bevestigen dat het probleem zich niet meer voortplant met de bypass op zijn plaats.

Alternatieve resolutie: Codex Configuration Workaround

Pas de Codex-configuratiwijzigingen toe waarnaar wordt verwezen in het GitHub-probleem om het volume van DNS-verzoeken die door de toepassing worden gegenereerd te verminderen.

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

Geavanceerde stappen voor probleemoplossing gebruikt

Deze diagnostische stappen werden uitgevoerd om de oorzaak te identificeren.

1.- Schakel het loggen van een sok in:

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

2.- Reproduceer het probleem en verzamel de DART-bundel onmiddellijk na het falen.

3.- Schakel uitgebreide logboekregistratie uit:

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

4.- Maximale foutopsporingslogboekregistratie voor SWG inschakelen. SWGConfigOverride.json-bestand met inhoud maken:

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

Opslaan op /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- Schakel RSM-traceringslogboeken voor DNS in. Maak force_log_level.plist bestand met inhoud:

```
<?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>
```

Opslaan in /opt/cisco/secureClient/umbrella/data.

Oorzaak

Het kernprobleem houdt verband met het gedrag van de Codex-applicatie, dat een zeer groot

aantal DNS-verzoeken genereert. Wanneer chatgpt.com niet wordt omzeild, worden deze verzoeken effectief gedupliceerd door de Cisco Secure Client, waardoor een DNS-storm ontstaat die leidt tot een hoog CPU-gebruik en een sockkernel-stuurprogramma instabiliteit.

Het probleem doet zich voor omdat:

- Codex genereert talrijke DNS-query's naar chatgpt.com tijdens de werking.
- Zonder bypass-configuratie onderschept en dupliceert Secure Client deze verzoeken.
- Het grote aantal dubbele DNS-aanvragen zorgt ervoor dat de stuurprogramma's crashen.
- De instabiliteit van de stuurprogramma's leidt tot uitval van de paraplusonde en de overgang naar de failopen toestand.

Wanneer chatgpt.com wordt omzeild of de Codex-oplossing wordt toegepast, treedt deze duplicatie niet op en wordt het probleem niet meer gereproduceerd. Het probleem heeft gevolgen voor zowel Umbrella-only- als ZTNA SIA-configuraties, wat aangeeft dat het probleem eerder binnen het verkeersregelingsmechanisme ligt dan binnen een specifieke module.

Gerelateerde inhoud

- [Problemen oplossen met de zwervende module voor beveiligde toegang](#)
- [Problemen oplossen en basisinformatie verzamelen](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.