

Il modulo Secure Client Umbrella diventa inattivo a causa di una tempesta DNS dell'applicazione Codex

Sommario

Problema

Più utenti su macOS sperimentano il modulo roaming Cisco Secure Client Umbrella in transizione intermittente verso uno stato inattivo (fail-open). Durante questi periodi, le richieste DNS, inclusi i comandi nslookup avviati dal terminale, non riescono a raggiungere il livello di rete, compromettendo la capacità degli utenti di risolvere i domini e di accedere alle risorse basate su Internet.

Il problema si manifesta con ripetuti errori di probe nei log di Umbrella, che mostrano messaggi come:

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

L'analisi ha rivelato che il driver della batteria si blocca durante la stessa finestra di errore quando Umbrella diventa inattiva. Il problema si osserva più frequentemente quando gli utenti utilizzano attivamente applicazioni Codex e AI Assistant, con un elevato volume di tentativi di connessione a chatgpt.com subito dopo l'invio dei comandi a CODEX.

Ambiente

- Cisco Secure Client versioni 5.1.13, 5.1.16, 5.1.17
- macOS (osservate più versioni)

- Modulo roaming Umbrella abilitato
- Modulo ZTNA/SIA (Secure Internet Access) abilitato
- Applicazione Codex in uso
- Utenti che lavorano da diverse reti (casa, ufficio, diversi ISP)

Risoluzione

Il problema è stato risolto implementando configurazioni di bypass del dominio per impedire la duplicazione delle richieste DNS. Gli approcci descritti nelle sezioni successive sono stati convalidati.

Risoluzione principale: Bypass dominio

- Passaggio 1: Aggiungere chatgpt.com all'elenco di esclusione nella configurazione di Cisco Secure Access. In questo modo si impedisce al client sicuro di duplicare le richieste DNS generate dall'applicazione Codex, eliminando la tempesta DNS che causa l'instabilità del driver.
- Passaggio 2: Verificare la configurazione di bypass. Provare la funzionalità Codex per verificare che il problema non si riproduca più con il bypass in posizione.

Risoluzione alternativa: Soluzione alla configurazione del codex

Applicare le modifiche alla configurazione del codice a cui si fa riferimento nel problema GitHub per ridurre il volume delle richieste DNS generate dall'applicazione.

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

Procedure avanzate di risoluzione dei problemi utilizzate

Queste operazioni diagnostiche sono state eseguite per identificare la causa principale.

1.- Abilitare la registrazione dettagliata delle scorte:

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

2.- Riprodurre il problema e raccogliere il pacchetto DART subito dopo il guasto.

3.- Disabilitare la registrazione dettagliata:

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

4.- Abilitare la registrazione di debug massima per SWG. Creare il file SWGConfigOverride.json con il seguente contenuto:

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

Salvare in /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- Abilitare i registri di traccia RSM per DNS. Creare il file force_log_level.plist con il contenuto:

```
<?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>
```

Salva in /opt/cisco/secureclient/umbrella/data.

Causa

Il problema principale è correlato al comportamento dell'applicazione Codex, che genera un volume molto elevato di richieste DNS. Quando chatgpt.com non viene ignorato, queste richieste

vengono duplicate in modo efficace da Cisco Secure Client, creando una tempesta DNS che determina un elevato utilizzo della CPU e l'instabilità del driver del kernel.

Il problema si verifica perché:

- Codex genera numerose query DNS in chatgpt.com durante il funzionamento.
- Senza ignorare la configurazione, Secure Client intercetta e duplica queste richieste.
- L'elevato volume di richieste DNS duplicate provoca l'arresto anomalo del driver di stack.
- L'instabilità del driver determina errori del probe Umbrella e la transizione allo stato di apertura in caso di errore.

Quando si ignora chatgpt.com o si applica la soluzione alternativa del codice, questa duplicazione non viene eseguita e il problema non si riproduce più. Il problema interessa sia le configurazioni SIA Umbrella-only che ZTNA, indicando che il problema si trova all'interno del meccanismo di gestione del traffico piuttosto che in un modulo specifico.

Contenuto correlato

- [Risoluzione dei problemi relativi al modulo Secure Access Roaming](#)
- [Risoluzione dei problemi e raccolta di informazioni di base](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).