CRYPTO_INTERNAL_ERROR durante i download sicuri di Google Drive

Sommario

Problema

I file crittografati di Google Sheets non si aprono quando vi si accede tramite Cisco Secure Access con la decrittografia del traffico abilitata. Gli utenti incontrano CRYPTO_INTERNAL_ERROR durante i download sicuri di Google Drive. Questo problema si verifica in modo specifico quando l'ispezione di Secure Web Gateway (SWG) è attiva, in quanto le intestazioni Range vengono ignorate durante il processo di decrittografia e ispezione, causando interferenze con il meccanismo di download sicuro di Google.

Il problema interessa gli ambienti che utilizzano l'implementazione di RAVPN+ZTA e influisce sull'accesso a Google Sheets crittografati per grandi gruppi di utenti.

Ambiente

- Tecnologia: Cisco Secure Access (supporto della soluzione)
- Sottotecnologia: Accesso sicuro
- Implementazione: RAVPN+ZTA (VPN ad accesso remoto + accesso con trust zero)
- Componente interessato: Profilo ZTA
- Domini interessati: clients6.google.com e altri domini relativi a Google Drive

Risoluzione

La risoluzione prevede l'implementazione di soluzioni temporanee durante il monitoraggio delle

correzioni permanenti lato fornitore.

Gli approcci delineati nelle sezioni successive sono stati convalidati per ripristinare l'accesso ai Google Sheets criptati.

Opzioni di soluzione temporanea

Opzione 1: Disabilita decrittografia traffico

Disabilitare completamente la decrittografia del traffico per i gruppi di utenti o i criteri interessati. In questo modo viene ripristinato l'accesso a Google Sheets ma vengono rimosse tutte le funzionalità di ispezione della sicurezza basate sulla decrittografia.

Opzione 2: Escludi i domini di Google Drive dalla decrittografia

Aggiungere i domini relativi a Google Drive all'elenco da non decrittografare nella configurazione dei criteri di accesso sicuro:

- clients6.google.com
- Altri domini relativi a Google Drive identificati nell'analisi del traffico

Questo approccio mantiene la decrittografia per il traffico di altro tipo, consentendo al contempo a Google Sheets di funzionare normalmente. Tuttavia, questa soluzione offre il compromesso tra la disabilitazione della funzionalità di blocco del caricamento di Google Drive del CASB per i domini esclusi.

Analisi e monitoraggio tecnici

L'analisi di Cisco ha confermato che l'ispezione di Secure Web Gateway ignora le intestazioni dell'intervallo per consentire un'analisi completa della sicurezza del contenuto dei file. Questo comportamento interferisce con il processo di download sicuro di Google Drive, che si basa sulle

intestazioni Range per un corretto flusso di decrittografia.

Google ha riconosciuto il problema e ha identificato che il comportamento del proxy (incluso Cisco Umbrella/proxy di rete) interferisce con le richieste di download sicuro di Google Drive rimuovendo o riscrivendo le intestazioni dell'intervallo. In questo modo viene forzato un download di file completo che interrompe il meccanismo di decrittografia di Google. Google sta sviluppando una soluzione sul lato client, anche se non è stato fornito un tempo stimato di arrivo.

Considerazioni sull'implementazione

Le organizzazioni che implementano le soluzioni alternative devono tenere conto delle implicazioni relative alla sicurezza:

- Valutare il rischio di esclusione dei domini di Google Drive dall'ispezione della decrittografia.
- Rivedere i criteri CASB che possono essere interessati dalle esclusioni di dominio.
- Documentare la natura temporanea della soluzione alternativa per future revisioni delle policy.
- Monitoraggio degli aggiornamenti di Google relativi allo sviluppo di correzioni lato client.

Causa

La causa principale è un problema di compatibilità tra il comportamento di ispezione Cisco Secure Access SWG e il meccanismo di download sicuro di Google Drive.

In particolare:

L'ispezione di Cisco Secure Web Gateway ignora le intestazioni dell'intervallo durante il processo di decrittografia e analisi della sicurezza per garantire un'analisi completa dei file. Tuttavia, l'accesso ai file crittografati di Google Drive si basa sulle intestazioni Range per gestire correttamente il flusso di decrittografia per i download sicuri. Quando queste intestazioni vengono rimosse o modificate durante il processo di ispezione del proxy, la decrittografia lato client di Google non riesce, generando CRYPTO_INTERNAL_ERROR.

Ciò rappresenta un'incompatibilità fondamentale tra i requisiti di ispezione della sicurezza

(scansione completa dei file) e il meccanismo di consegna dei file crittografati di Google (download protetti basati su intervalli).

Contenuto correlato

- 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).