CRYPTO_INTERNAL_ERROR durante las descargas seguras de Google Drive

Contenido

Problema

Los archivos cifrados de Google Sheets no se pueden abrir cuando se accede a ellos a través de Cisco Secure Access con el descifrado de tráfico habilitado. Los usuarios encuentran un ERROR CRYPTO_INTERNAL_ERROR durante las descargas seguras de Google Drive. Este problema se produce específicamente cuando la inspección de Secure Web Gateway (SWG) está activa, ya que los encabezados Range se ignoran durante el proceso de descifrado e inspección, lo que provoca interferencias con el mecanismo de descarga segura de Google.

El problema afecta a los entornos que utilizan la implementación de RAVPN+ZTA y afecta al acceso a las hojas de Google cifradas para grandes poblaciones de usuarios.

Entorno

- Tecnología: Cisco Secure Access (Asistencia para soluciones)
- Subtecnología: Acceso seguro
- Instrumentación: RAVPN+ZTA (VPN de acceso remoto + acceso de confianza cero)
- Componente afectado: Perfil ZTA
- Dominios afectados: clients6.google.com y otros dominios relacionados con Google Drive

Resolución

La resolución implica la implementación de soluciones temporales mientras se supervisa la

corrección permanente por parte del proveedor.

Los enfoques descritos en las siguientes secciones se han validado para restaurar el acceso a las Hojas de cálculo de Google cifradas.

Opciones temporales de solución alternativa

Opción 1: Deshabilitar descifrado de tráfico

Deshabilitar completamente el descifrado de tráfico para los grupos de usuarios o políticas afectados. Esto restaura el acceso a Google Sheets, pero elimina todas las funciones de inspección de seguridad basadas en descifrado.

Opción 2: Excluir dominios de Google Drive del descifrado

Agregue dominios relacionados con Google Drive a la lista de no descifrar en la configuración de la directiva de acceso seguro:

- clients6.google.com
- Otros dominios relacionados con Google Drive identificados en el análisis del tráfico

Este enfoque mantiene el descifrado para el resto del tráfico, a la vez que permite que las hojas de Google funcionen con normalidad. Sin embargo, esta solución alternativa tiene el inconveniente de deshabilitar la funcionalidad de bloqueo de carga de CASB Google Drive para los dominios excluidos.

Análisis técnico y supervisión

El análisis de Cisco confirmó que la inspección del gateway web seguro ignora los encabezados de rango para habilitar el análisis de seguridad integral del contenido del archivo. Este comportamiento interfiere con el proceso de descarga segura de Google Drive, que se basa en

encabezados Range para un flujo de descifrado adecuado.

Google ha reconocido el problema e identificado que el comportamiento de proxy (incluido Cisco Umbrella/proxy de red) interfiere con las solicitudes de descarga segura de Google Drive al eliminar o volver a escribir los encabezados Range. Esto obliga a una descarga de archivos completos que rompe el mecanismo de descifrado de Google. Google está desarrollando una solución en el lado del cliente, aunque no se ha proporcionado una hora estimada de llegada.

Consideraciones de Implementación

Las organizaciones que implementan las soluciones alternativas deben tener en cuenta las implicaciones de seguridad:

- Evaluar el riesgo de excluir los dominios de Google Drive de la inspección de descifrado.
- Revise las políticas CASB que pueden verse afectadas por las exclusiones de dominio.
- Documentar el carácter temporal de la solución alternativa para futuras revisiones de políticas.
- Supervisar las actualizaciones de Google con respecto a su desarrollo de soluciones en el lado del cliente.

Causa

La causa principal es un problema de compatibilidad entre el comportamiento de inspección SWG de Cisco Secure Access y el mecanismo de descarga segura de Google Drive.

Específicamente:

La inspección de Cisco Secure Web Gateway omite los encabezados de rango durante el proceso de descifrado y análisis de seguridad para garantizar un análisis de archivos completo. Sin embargo, el acceso a archivos cifrados de Google Drive se basa en encabezados Range para gestionar correctamente el flujo de descifrado para realizar descargas seguras. Cuando estos encabezados se eliminan o modifican durante el proceso de inspección de proxy, el descifrado del lado del cliente de Google falla, lo que resulta en CRYPTO_INTERNAL_ERROR.

Esto representa una incompatibilidad fundamental entre los requisitos de inspección de seguridad (análisis completo de archivos) y el mecanismo de entrega de archivos cifrados de Google (descargas seguras basadas en intervalos).

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).