CRYPTO_INTERNAL_ERROR bei Google Drive Secure Downloads

Inhalt

Problem

Verschlüsselte Google Sheets-Dateien können nicht geöffnet werden, wenn auf sie über Cisco Secure Access mit aktivierter Datenverkehrsentschlüsselung zugegriffen wird. Benutzer stoßen beim sicheren Herunterladen von Google Drive auf einen CRYPTO_INTERNAL_ERROR. Dieses Problem tritt insbesondere dann auf, wenn die SWG-Überprüfung (Secure Web Gateway) aktiv ist, da Range-Header während des Entschlüsselungs- und Überprüfungsprozesses ignoriert werden, was zu Interferenzen mit dem sicheren Google-Downloadmechanismus führt.

Das Problem betrifft Umgebungen, in denen RAVPN+ZTA implementiert ist, und den Zugriff auf verschlüsselte Google Sheets für große Nutzerzahlen.

Umwelt

- Technologie: Cisco Secure Access (Lösungssupport)
- Untertechnologie: Sicherer Zugriff
- Implementierung: RAVPN + ZTA (Remote Access VPN + Zero Trust Access)
- Betroffene Komponente: ZTA-Profil
- Betroffene Domänen: clients6.google.com und andere Google Drive-bezogene Domains

Auflösung

Die Lösung beinhaltet die Implementierung temporärer Workarounds und die Überwachung auf

permanente anbieterseitige Korrekturen.

Die in den nächsten Abschnitten beschriebenen Ansätze wurden validiert, um den Zugriff auf verschlüsselte Google Sheets wiederherzustellen.

Temporäre Workaround-Optionen

Option 1: Datenverkehrsentschlüsselung deaktivieren

Deaktivieren Sie die Entschlüsselung des Datenverkehrs für die betroffenen Benutzergruppen oder Richtlinien vollständig. Dadurch wird der Zugriff auf Google Sheets wiederhergestellt, aber alle Funktionen für die entschlüsselungsbasierte Sicherheitsprüfung werden entfernt.

Option 2: Google Drive-Domänen von Entschlüsselung ausschließen

Fügen Sie der Liste "Nicht entschlüsseln" in der Konfiguration der Richtlinie für sicheren Zugriff Domänen hinzu, die sich auf Google Drive beziehen:

- clients6.google.com
- Andere Google Drive-bezogene Domänen, wie in der Datenverkehrsanalyse identifiziert

Dieser Ansatz hält die Entschlüsselung für anderen Datenverkehr aufrecht, während Google Sheets normal funktionieren. Diese Problemumgehung hat jedoch den Nachteil, dass die Upload-Blockierungsfunktion von CASB Google Drive für die ausgeschlossenen Domänen deaktiviert wird.

Technische Analyse und Überwachung

Die Analyse von Cisco hat bestätigt, dass die Secure Web Gateway-Überprüfung Range-Header ignoriert, um umfassende Sicherheits-Scans von Dateiinhalten zu ermöglichen. Dieses Verhalten stört den sicheren Download-Prozess von Google Drive, der auf Range-Headern für einen

ordnungsgemäßen Entschlüsselungsfluss beruht.

Google hat das Problem bestätigt und festgestellt, dass das Proxy-Verhalten (einschließlich Cisco Umbrella/Netzwerk-Proxy) die sicheren Download-Anforderungen von Google Drive beeinträchtigt, indem Range-Header entfernt oder umgeschrieben werden. Dies erzwingt einen vollständigen Download, der den Google-Entschlüsselungsmechanismus unterbricht. Google entwickelt derzeit eine kundenseitige Fehlerbehebung, es wurde jedoch keine geschätzte Ankunftszeit angegeben.

Überlegungen zur Implementierung

Organisationen, die Workarounds implementieren, sollten die Auswirkungen auf die Sicherheit berücksichtigen:

- Bewerten Sie das Risiko, Google Drive-Domänen von der Entschlüsselungsprüfung auszuschließen.
- Überprüfen Sie die CASB-Richtlinien, die von Domänenausschlüssen betroffen sein können.
- Dokumentieren Sie die temporäre Natur des Workaround für künftige politische Überprüfungen.
- Überwachen Sie, um Updates von Google bezüglich ihrer clientseitigen Fix-Entwicklung zu erhalten.

Ursache

Die Ursache liegt in einem Kompatibilitätsproblem zwischen dem Überprüfungsverhalten der Cisco Secure Access SWG und dem sicheren Downloadmechanismus von Google Drive.

Konkret:

Bei der Cisco Secure Web Gateway-Prüfung werden Range-Header während des Entschlüsselungs- und Sicherheits-Scanvorgangs ignoriert, um eine vollständige Dateianalyse sicherzustellen. Der verschlüsselte Dateizugriff über Google Drive verlässt sich jedoch auf Range-Header, um den Entschlüsselungsfluss für sichere Downloads ordnungsgemäß zu handhaben. Wenn diese Header während der Proxy-Überprüfung entfernt oder geändert werden, schlägt die Client-seitige Entschlüsselung von Google fehl, was zu CRYPTO_INTERNAL_ERROR führt.

Dies stellt eine grundlegende Inkompatibilität zwischen den Anforderungen an die Sicherheitsüberprüfung (vollständiges Scannen von Dateien) und dem Mechanismus für die verschlüsselte Dateibereitstellung von Google (entfernungsbasierte sichere Downloads) dar.

Verwandte Inhalte

- 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.