CRYPTO_INTERNAL_ERROR tijdens Google Drive Secure Downloads

Inhoud

uitgifte

Gecodeerde Google Sheets-bestanden kunnen niet worden geopend wanneer ze worden geopend via Cisco Secure Access met verkeersdecodering ingeschakeld. Gebruikers stuiten op een CRYPTO_INTERNAL_ERROR tijdens beveiligde downloads van Google Drive. Dit probleem treedt specifiek op wanneer de Secure Web Gateway (SWG)-inspectie actief is, omdat Range-headers worden genegeerd tijdens het decoderings- en inspectieproces, wat leidt tot interferentie met het beveiligde downloadmechanisme van Google.

Het probleem beïnvloedt omgevingen met RAVPN + ZTA-implementatie en heeft invloed op de toegang tot gecodeerde Google Sheets voor grote gebruikersgroepen.

milieu

- Technologie: Cisco Secure Access (ondersteuning voor oplossingen)
- Subtechnologie: veilige toegang
- Implementatie: RAVPN+ZTA (Remote Access VPN + Zero Trust Access)
- Betrokken onderdeel: ZTA-profiel
- Betrokken domeinen: clients6.google.com en andere Google Drive-gerelateerde domeinen

resolutie

De resolutie gaat over het implementeren van tijdelijke tijdelijke oplossingen, terwijl er wordt

gemonitord op permanente oplossingen aan de kant van de leverancier.

De benaderingen die in de volgende secties worden beschreven, zijn gevalideerd om de toegang tot gecodeerde Google Sheets te herstellen.

Opties voor tijdelijke tijdelijke tijdelijke oplossing

Optie 1: Verkeersdecodering uitschakelen

Verkeersdecodering voor de betrokken gebruikersgroepen of beleidsregels volledig uitschakelen. Hiermee wordt de toegang tot Google Sheets hersteld, maar worden alle op decodering gebaseerde beveiligingsinspectiemogelijkheden verwijderd.

Optie 2: Google Drive-domeinen uitsluiten van decodering

Voeg Google Drive-gerelateerde domeinen toe aan de lijst met niet-ontsleutelen in de beleidsconfiguratie voor beveiligde toegang:

- clients6.google.com
- Andere Google Drive-gerelateerde domeinen zoals geïdentificeerd in verkeersanalyse

Deze aanpak handhaaft decryptie voor ander verkeer, terwijl Google Sheets normaal kan functioneren. Deze oplossing heeft echter de wisselwerking van het uitschakelen van de CASB Google Drive-uploadblokfunctionaliteit voor de uitgesloten domeinen.

Technische analyse en monitoring

De Cisco-analyse bevestigde dat Secure Web Gateway-inspectie Range-headers negeert om uitgebreide beveiligingsscans van bestandsinhoud mogelijk te maken. Dit gedrag interfereert met het beveiligde downloadproces van Google Drive, dat afhankelijk is van Range-headers voor een goede decoderingsstroom.

Google heeft het probleem erkend en vastgesteld dat proxygedrag (inclusief Cisco Umbrella / network proxy) interfereert met beveiligde downloadverzoeken van Google Drive door Range-headers te verwijderen of te herschrijven. Dit dwingt een full-file download die het Google decryptie mechanisme breekt. Google is bezig met het ontwikkelen van een client-side fix, hoewel er geen geschatte tijd van aankomst is verstrekt.

Overwegingen met betrekking tot de uitvoering

Organisaties die de workarounds implementeren, moeten rekening houden met de veiligheidsimplicaties:

- Evalueer het risico van het uitsluiten van Google Drive-domeinen van decryptie-inspectie.
- Controleer het CASB-beleid dat kan worden beïnvloed door de domeinuitsluitingen.
- Documenteer de tijdelijke aard van de tijdelijke oplossing voor toekomstige beleidsherzieningen.
- Monitor voor updates van Google met betrekking tot hun client-side fix ontwikkeling.

Oorzaak

De hoofdoorzaak is een compatibiliteitsprobleem tussen het inspectiegedrag van Cisco Secure Access SWG en het beveiligde downloadmechanisme van Google Drive.

Concreet:

Cisco Secure Web Gateway-inspectie negeert Range-headers tijdens het decryptie- en beveiligingsscanproces om een volledige bestandsanalyse te garanderen. De gecodeerde bestandstoegang van Google Drive is echter afhankelijk van Range-headers om de decoderingsstroom voor veilige downloads goed aan te kunnen. Wanneer deze headers worden verwijderd of gewijzigd tijdens het proxy-inspectieproces, mislukt de decodering aan de clientzijde van Google, wat resulteert in de CRYPTO_INTERNAL_ERROR.

Dit is een fundamentele incompatibiliteit tussen de vereisten voor beveiligingsinspecties (volledige bestandsscanning) en het versleutelde bestandsleveringsmechanisme van Google (op bereik gebaseerde beveiligde downloads).

Gerelateerde inhoud

- 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.