

Problemen oplossen met de Health Check van de module Foutcode mislukt in Secure Access XDR-integratie

Inhoud

uitgifte

De integratie van Cisco Secure Access met XDR mislukt met een HTTP 431 "Request Header Fields Too Large"-fout tijdens de controlefase. De integratie had eerder met succes gewerkt, maar begon plotseling te falen met deze fout bij het proberen om de verbinding tot stand te brengen met behulp van API-sleutels gegenereerd vanuit het Cisco Secure Access-dashboard.

De specifieke foutmelding wordt weergegeven als:

<#root>

Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access

Deze fout voorkomt dat Secure Access-gegevens in XDR worden opgenomen, wat van invloed is op de zichtbaarheid van de beveiliging en de bewakingsmogelijkheden.

milieu

- Cisco Secure Access met Advantage-licentie
- Cisco XDR-abonnement
- Cisco Secure Access-tenant
- API-integratie met behulp van door Cisco Secure Access gegenereerde dashboardsleutels

- Vereiste API-scopes: onderzoeken > Alleen-lezen, rapporten > Alleen-lezen, implementaties > Alleen-lezen, beleid > Lezen/schrijven

resolutie

Het probleem is opgelost door de API-sleutel en het geheim opnieuw te genereren in Cisco Secure Access.

Volg deze stappen om de 431-fout op te lossen:

Stap 1: Nieuwe API-sleutels genereren

Navigeer naar het Cisco Secure Access-dashboard en maak nieuwe API-sleutels met de vereiste scopes:

- Onderzoeken: alleen-lezen
- Rapporten: alleen-lezen
- Implementaties: alleen-lezen
- Beleid: lezen/schrijven

Stap 2: Nieuwe sleutels toepassen op XDR-integratie

Vervang de bestaande API-sleutels in de XDR Secure Access-integratieconfiguratie door de nieuw gegenereerde sleutels.

Stap 3: Integratie verifiëren

Test de integratie om een succesvolle verbinding te bevestigen. De API-aanroepen moeten nu HTTP 200-antwoorden retourneren in plaats van de 431-fout.

Proactieve detectie en preventie

Om soortgelijke 431 fouten in de toekomst te identificeren en te voorkomen:

1.- Bij het debuggen via tools zoals Postman of browser console, controleer de grootte kolom voor verzoek headers. Als de headers van het verzoek 8 KB (8192 bytes) benaderen of overschrijden, veroorzaakt dit een 431-fout op API-gateways. Externe tools zoals jwt.io kunnen worden gebruikt om de OAuth-tokengrootte te verifiëren.

2.- Analyseer foutpatronen:

- Als de 431-fout onmiddellijk optreedt tijdens de eerste handdruk van een gezondheidscontrole, geeft dit aan dat de statische referenties het probleem zijn
- Als de 431-fout pas optreedt nadat de integratie enkele minuten heeft geduurd, wijst dit op het verzamelen van cookies tijdens latere herhalingen

best practices

Schakel cookie- of sessiepersistentie uit in de integratieclient/browser om accumulatie van de header-grootte te voorkomen.

Oorzaak

De HTTP 431-fout werd veroorzaakt doordat de specifieke API-sleutel en het geheime paar een ongewoon grote of misvormde autorisatieheader genereerden wanneer Base64 werd gecodeerd voor de standaard HTTP-autorisatieheader.

De cryptografische tekenreeksen in de initiële API-sleutel bevatten een reeks tekens die, wanneer gecodeerd, zijn uitgebreid tot een header die de API-gatewaylimieten heeft overschreden, wat resulteert in de afwijzing "Request Header Fields Too Large".

Toen de API-sleutel opnieuw werd gegenereerd, produceerde de nieuwe cryptografische tekenreeks een autorisatieheader van de juiste grootte. Het proces van het intrekken en genereren van een nieuwe sleutel heeft ook de context van het gecachte verzoek aan de kant

van de integratiemanager gewist, waardoor de header-grootte werd genormaliseerd.

Gerelateerde inhoud

- [Cisco Secure Access API-verificatie](#)
- [Cisco Secure Access-integratie in XDR](#)
- [HAR-logs verzamelen van XDR-console](#)
- [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.