

Fehlerbehebung: Integritätsprüfung des Moduls - Fehlercode bei XDR-Integration mit sicherem Zugriff fehlgeschlagen

Inhalt

Problem

Die Cisco Secure Access-Integration mit XDR schlägt während der Integritätsprüfung mit dem HTTP-431-Fehler "Request Header Fields Too Large" fehl. Die Integration funktionierte zuvor erfolgreich, aber plötzlich trat dieser Fehler auf, als versucht wurde, die Verbindung mithilfe von API-Schlüsseln herzustellen, die vom Cisco Secure Access Dashboard generiert wurden.

Die entsprechende Fehlermeldung wird angezeigt als:

<#root>

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

Dieser Fehler verhindert, dass Secure Access-Daten in XDR aufgenommen werden, was sich auf die Sicherheitstransparenz und die Überwachungsfunktionen auswirkt.

Umwelt

- Cisco Secure Access mit Advanced-Lizenz
- Cisco XDR-Abonnement
- Cisco Secure Access-Tenant
- API-Integration mit vom Cisco Secure Access Dashboard generierten Schlüsseln

- Erforderliche API-Bereiche: Investigate > Read-Only, Reports > Read-only, Deployments > Read-only, Policies > Read/Write

Auflösung

Das Problem wurde durch die Neugenerierung von API-Schlüssel und Schlüssel in Cisco Secure Access behoben.

Befolgen Sie diese Schritte, um den 431-Fehler zu beheben:

Schritt 1: Neue API-Schlüssel generieren

Navigieren Sie zum Cisco Secure Access-Dashboard, und erstellen Sie neue API-Schlüssel mit den erforderlichen Bereichen:

- Untersuchen: Schreibgeschützt
- Berichte: Schreibgeschützt
- Bereitstellungen: Schreibgeschützt
- Richtlinien: Lese-/Schreibzugriff

Phase 2: Anwendung neuer Schlüssel auf die XDR-Integration

Ersetzen Sie die vorhandenen API-Schlüssel in der XDR Secure Access-Integrationskonfiguration durch die neu generierten Schlüssel.

Schritt 3: Überprüfen der Integration

Testen Sie die Integration, um die erfolgreiche Verbindung zu bestätigen. Die API-Aufrufe müssen jetzt HTTP 200-Antworten zurückgeben, nicht mehr den 431-Fehler.

Proaktive Erkennung und Prävention

Um ähnliche 431 Fehler in der Zukunft zu erkennen und zu vermeiden:

1.- Beim Debuggen über Tools wie Postman oder Browserkonsole überprüfen Sie die Größenspalte für Anforderungskopfzeilen. Wenn die Request-Header 8 KB (8192 Byte) erreichen oder überschreiten, löst dies einen 431-Fehler auf API-Gateways aus. Externe Tools wie jwt.io können verwendet werden, um die Größe des OAuth-Tokens zu überprüfen.

2.- Analyse von Fehlermustern:

- Wenn der 431-Fehler unmittelbar während des ersten Handshakes einer Integritätsprüfung auftritt, weist dies darauf hin, dass die statischen Anmeldeinformationen das Problem darstellen
- Tritt der 431-Fehler erst nach einer mehrminütigen Integration auf, weist er auf eine Cookie-Akkumulation bei nachfolgenden Wiederholungen hin

Best Practices

Deaktivieren Sie die Dauerhaftigkeit von Cookies oder Sitzungen im Integrations-Client/Browser, um eine Anhäufung von Headergrößen zu verhindern.

Ursache

Der HTTP-431-Fehler wurde durch den spezifischen API-Schlüssel und das geheime Paar verursacht, die einen ungewöhnlich großen oder fehlerhaften Autorisierungsheader generierten, wenn Base64 für den Standard-HTTP-Autorisierungsheader codiert wurde.

Die kryptografischen Zeichenfolgen im ursprünglichen API-Schlüssel enthielten eine Sequenz von Zeichen, die sich bei der Codierung in eine Headergröße ausweiteten, die die API-Gateway-Grenzwerte überschreitete, was zur Ablehnung von "Request Header Fields Too Large" führte.

Wenn der API-Schlüssel neu generiert wurde, hat die neue kryptografische Zeichenfolge einen Autorisierungsheader in der richtigen Größe erzeugt. Durch das Widerrufen und Generieren eines

neuen Schlüssels wurde auch der im Cache gespeicherte Anforderungskontext auf Seite des Integrations-Managers gelöscht, wodurch die Headergröße normalisiert wurde.

Verwandte Inhalte

- [Cisco Secure Access API-Authentifizierung](#)
- [Cisco Secure Access Integration in XDR](#)
- [Sammeln von HAR-Protokollen von der XDR-Konsole](#)
- [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.