Beheben von Ereignissen mit sicherem Zugriff API Remote-Zugriff 403 Access Forbidden-Fehler

Inhalt

Problem

Beim Versuch, VPN-Remotezugriffsprotokolle mithilfe der Cisco Secure Access API-Endpunkte/Berichte/v2/Remotezugriffsereignisse abzurufen, erhalten Benutzer stets die Antwort "403 Access Forbidden", obwohl sie alle erforderlichen Bereiche aktiviert haben, einschließlich reports.granularevents:read. Das Problem tritt auf, wenn API-Aufrufe mit folgenden Parametern durchgeführt werden:

```
Authorization: Bearer <token>
Accept: application/json
Endpoint: https://api.sse.cisco.com/reports/v2/remote-access-events
Params: {"limit": 500, "from": "-6000minutes", "to": "now"}
HTTP status: 403
Events retrieved: 0
Access Forbidden
```

Der Fehler tritt auf, obwohl im API-Schlüssel mehrere Berichtsbereiche konfiguriert sind und andere API-Endpunkte ordnungsgemäß funktionieren. Benutzer berichten, dass sie erfolgreich auf andere Berichtsendpunkte zugreifen können, es jedoch speziell zu Autorisierungsproblemen mit dem Remotezugriffsereignisendpunkt kommen kann.

Umwelt

- Cisco Secure Access-API
- API-Endpunkt: /reports/v2/remote-access-events
- API-Schlüssel mit konfigurierten Bereichen: admin.vpn:read, admin.users:read, admin.alertrules:read, admin.warnt:read, admin.sentinel:read, reports.aggregations:read,

reports.granularevents:read, reports.malware:read, reports.incidents:read, reports.dlp.events:read
- Benutzer mit vollständigen Administratorberechtigungen im Secure Access-Portal
- API-Integration mit Überwachungssystemen

Auflösung

Das Problem wurde mithilfe des richtigen API-Bereichs für den Remotezugriffsereignisendpunkt behoben. Der dokumentierte Umfang und die tatsächlichen Implementierungsanforderungen unterscheiden sich für dieses spezifische Endgerät.

Ursachenanalyse

Die Untersuchung ergab eine Diskrepanz zwischen dem dokumentierten API-Umfang und der tatsächlichen Implementierung:

- Dokumentationsstatus: Der erforderliche Bereich ist reports.aggregations:read.
- Tatsächliche Implementierung: Die externe API-Gateway-ACL ordnet Berichte/v2/Remotezugriffsereignisse reports.utilities:read zu.

Ergebnisse der Bereichstests

Der Test hat dieses Bereichsverhalten bestätigt:

```
Token Scope: reports.aggregations:read
GET /reports/v2/remote-access-events
Response: 403

Token Scope: reports.utilities:read
GET /reports/v2/remote-access-events
Response: 200

Token Scope: reports.* (All Reports)
GET /reports/v2/remote-access-events
Response: 200
```

Implementierung der Lösung

Um den 403 Access Forbidden-Fehler zu beheben, konfigurieren Sie den API-Schlüssel mit dem richtigen Gültigkeitsbereich:

Schritt 1: Zugriff auf API-Schlüsselverwaltung.

Navigieren Sie im Dashboard für sicheren Zugriff zu Admin > API Keys (Admin > API-Schlüssel).

Phase 2: Neuen API-Schlüssel erstellen.

Klicken Sie auf API-Schlüssel hinzufügen (+) und konfigurieren Sie:

- API-Schlüsselname
- Beschreibung (optional)
- Gewünschtes Ablaufdatum

Schritt 3: Konfigurieren Sie den korrekten Bereich.

Aktivieren Sie im Abschnitt Bereiche die Funktion reports.utilities:read für Remotezugriffsereignisse.

Schritt 4: Träger-Token generieren.

Erstellen Sie ein neues Trägertoken mithilfe des OAuth2-Clientanmeldeinformationsflusses mit dem aktualisierten API-Schlüssel.

Schritt 5: Test-API-Aufruf.

Wiederholen Sie den API-Aufruf mit dem Befehlsformat curl:

```
curl -L --request GET \
--url 'https://api.sse.cisco.com/reports/v2/remote-access-events?limit=10&from=-60minutes&to=now' \
--header 'Authorization: Bearer <Bearer token>' \
--header 'Accept: application/json'
```

Schritt 6: Überprüfen der Auflösung.

Durch Bestätigen des API-Aufrufs wird der HTTP 200-Status zurückgegeben und die erwarteten Remotezugriffsereignisdaten abgerufen.

Ursache

Die Ursache hierfür liegt in einer Diskrepanz zwischen den Anforderungen des dokumentierten API-Bereichs und der tatsächlichen Implementierung in der externen API-Gateway-ACL. In der öffentlichen Dokumentation von Cisco für GET /reports/v2/remote-access-events wird fälschlicherweise angegeben, dass der erforderliche Zugriffsbereich reports.aggregations:read ist, wenn die eigentliche Implementierung reports.utilities:read erfordert. Diese Diskrepanz führt zu Authentifizierungsfehlern, selbst wenn Benutzer glauben, die richtigen Berechtigungen auf Basis der offiziellen Dokumentation konfiguriert zu haben.

Verwandte Inhalte

- Cisco Secure Access API - Remote Access-Ereignisse abrufen
- 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.