تكوين ملفات تعريف أمان الوصول الآمن API المتقدمة

المحتويات

مسألة

عند محاولة تكوين ملفات تعريف أمان الوصول الآمن من Cisco من خلال واجهة برمجة تطبيقات (API) العامة، يواجه المستخدمون قيود لا يمكن فيها إنشاء ملف تعريف أساسي إلا باستخدام الإعدادات الافتراضية. لا تكشف واجهة برمجة التطبيقات (API) عن خيارات التكوين متعددة المستويات لميزات الأمان المتقدمة، بما في ذلك:

- إعدادات فك تشفير TLS
- عناصر التحكم في الإنفاذ من فئة التهديدات
- حظر نوع الملف وتفتيشه
- إعدادات فحص البرامج الضارة

يبلغ المستخدمون عن تلقي أخطاء "403 ممنوع" عند محاولة تكوين إعدادات فك التشفير من خلال إستدعاءات واجهة برمجة التطبيقات (API) القياسية. يبدو أن نقاط نهاية واجهة برمجة التطبيقات العامة الموثقة تفتقر إلى معلمات تكوين ملف تعريف الأمان التفصيلي المتوفرة من خلال واجهة واجهة المستخدم الرسومية، مما يحد من إمكانيات الإدارة البرمجية.

البيئة

- النظام الأساسي للوصول الآمن من Cisco
- ملفات تعريف الأمان لتنفيذ واجهة برمجة التطبيقات (API)
- تأثرت جميع إصدارات البرامج
- نقاط النهاية لوثائق واجهة برمجة التطبيقات العامة

قرار

تتوفر قدرات تكوين ملف تعريف الأمان المتقدمة من خلال واجهة برمجة تطبيقات Cisco Secure Access API، ولكنها تتطلب نهج تنفيذ محددة واتفاقيات تسمية الحقول التي تختلف عن أمثلة واجهة برمجة التطبيقات العامة الموثقة. تتطرق خطوات الحل هذه لكل منطقة تكوين:

سير عمل إنشاء ملف تعريف الأمان الأساسي

يتبع سير العمل المناسب لإنشاء توصيفات تأمين بإعدادات متقدمة عملية من خطوتين:

الخطوة 1: قم بإنشاء ملف تعريف التأمين الأساسي باستخدام POST.

```
POST /api/v1/security-profiles
{
  "name": "profile_name",
  "description": "profile_description"
}
```

الخطوة 2: قم بتكوين الخيارات المتقدمة باستخدام PUT مع معرف التوصيف.

```
PUT /api/v1/security-profiles/{profile_id}
{
  "advanced_settings": {
    "decryption_settings": {...},
    "file_settings": {...},
    "threat_settings": {...}
  }
}
```

تكوين حظر نوع الملف و فحص الملفات

يمكن تكوين فحص الملفات وحظر نوع الملفات باستخدام أسماء حقول API هذه ضمن طلب PUT:

- FileEngines - التحكم في إمكانيات فحص الملفات.
- FileTypeControlStatus - تمكين حظر نوع الملف أو تعطيله.

مثال على التكوين لإعدادات الملف:

```
{
"fileEngines": "enabled",
"fileTypeControlStatus": "active",
"blockedFileTypes": ["exe", "zip", "rar"]
}
```

تكوين فك تشفير TLS

يتطلب تكوين فك تشفير TLS الرجوع إلى معرف قائمة عدم فك التشفير بدلا من إستخدام نقطة نهاية POST مخصصة. يتم تنفيذ التكوين من خلال طلب واجهة برمجة تطبيقات PUT باستخدام هذا النهج:

الخطوة 1: التعرف على معرف قائمة عدم فك التشفير من التكوين الحالي.

الخطوة 2: قم بمرجع معرف القائمة في طلب واجهة برمجة تطبيقات PUT.

```
{
"seetingGroupBypassInspectionGroupID": "do_not_decrypt_list_id",
"decryptionEnabled": true
}
```

قد يؤدي هذا إلى حل الخطأ "403 ممنوع" الذي يحدث عند محاولة تكوين فك التشفير من خلال طرق واجهة برمجة التطبيقات الأخرى.

تكوين فئة التهديد

يتوفر تكوين فئة التهديد من خلال نقطة نهاية API غير موثقة يمكن الوصول إليها بعد تمكين فك التشفير النافذ. تسمح نقطة النهاية بالتحكم في فئة التهديد متعددة المستويات لكنها تتطلب تكوين ملف تعريف الأمان بشكل صحيح باستخدام إعدادات فك التشفير أولا.

مرجع اسم حقل API

يقوم هذا الجدول بتعيين ميزات ملف تعريف الأمان الشائع لأسماء حقول API المطابقة لها:

الميزة	اسم حقل API	الوصف
فك تشفير TLS	seetingGroupBypassInspectionGroupID	تعرف مجموعة المراجع بفك تشفير ال القائمة
فحص الملفات	FileEngines	التحكم في إمكانيات فحص الملفات
حظر نوع الملف	fileTypeControlStatus	تمكين تقييدات نوع الملف

السبب

ويعزى هذا القيد في المقام الأول إلى عدم اكتمال وثائق واجهة برمجة التطبيقات واتفاقيات تسمية الحقول غير البديهية بدلا من القيود الوظيفية الفعلية. توجد إمكانات تكوين ملف تعريف الأمان المتقدم داخل واجهة برمجة التطبيقات (API) ولكن يتم تنفيذها باستخدام:

- أسماء الحقول غير الواضحة التي تختلف عن مصطلحات واجهة المستخدم الرسومية
- سير عمل من خطوتين (POST للإنشاء، PUT للتكوين المتقدم)
- التبعيات على كائنات التكوين الموجودة (مثل قوائم عدم فك التشفير)
- نقاط نهاية API غير موثقة لميزات معينة

لا تكشف وثائق واجهة برمجة التطبيقات (API) العامة تفاصيل التنفيذ هذه بشكل واضح، مما يؤدي إلى تصور قيود واجهة برمجة التطبيقات (API) عندما تكون الوظيفة متاحة بالفعل من خلال النهج البديلة.

المحتوى ذي الصلة

- [وثائق واجهة برمجة التطبيقات (API) لملفات تعريف أمان الوصول الآمن من Cisco]
- [الدعم الفني والتنزيلات من Cisco]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).