أستكشاف أخطاء SWG SAML Authentication Cookie البديلة للوصول الآمن

المحتويات

مسألة

فشل مصادقة تجربة الوصول الآمن من Cisco للمستخدمين الذين يصلون إلى تطبيقات الويب عندما تقوم التطبيقات بإعادة التوجيه عبر المجالات أو إحضار موارد من مجالات متعددة ذات صلة. يظهر الإصدار كما يلي:

- فشل تهيئة تطبيقات ويب بشكل صحيح بعد مصادقة SAML.
- طلبات الموارد عبر المجال (خطأ CORS) التي يتم حظرها بواسطة قواعد الرفض الافتراضية.
- سجلات النشاط التي تظهر الطلبات المنسوبة إلى هوية الشبكة أو النفق بدلا من هوية المستخدم المصدق عليها.
- تظهر أخطاء نهج CORS في وحدة تحكم المستعرض للطلبات المعاد توجيهها.
- التطبيقات التي تعمل بشكل صحيح على الأجهزة المدارة عند إستخدام بدائل IP ولكنها تفشل في بيئات سطح المكتب الافتراضية من Citrix باستخدام بدائل الكعك.

تحدث المشكلة تحديدا عند إستخدام مصادقة ملف تعريف الارتباط البديلة في البيئات الافتراضية، حيث تفقد الطلبات التي تمت إعادة توجيهها تعيين ملف تعريف الارتباط من المستخدم إلى ملف تعريف الارتباط أثناء عمليات إحضار موارد عبر المجال.

البيئة

- الوصول الآمن من Cisco مع مصادقة SAML التي تم تكوينها
- تم تمكين مصادقة بديل ملفات تعريف الارتباط لبيئات سطح المكتب الظاهرية من Citrix

- مصادقة بديل IP المستخدمة للأجهزة الفعلية
- تطبيقات ويب التي تقوم بإعادة توجيه عبر المجال (خطأ CORS في سجلات وحدة التحكم لأداة مطور الويب)
- بيئة مختلطة مع البنية الأساسية الفعلية والافتراضية للكمبيوتر المكتبي

قرار

يتم حل المشكلة عن طريق تنفيذ تجاوز IP البديل لنطاقات الشبكة المتأثرة، مما يسمح بتخصيص هوية المستخدم بشكل صحيح حتى أثناء عمليات إعادة التوجيه عبر المجالات.

الخطوة 1: انتقل إلى تكوين بديل IP

قم بالوصول إلى لوحة معلومات الوصول الآمن من Cisco وتصفح للاتصال > المستخدمين والمجموعات > إدارة التكوين > الإعدادات المتقدمة > إستبدال IP.

الخطوة 2: تمكين تجاوز الشبكة الداخلية

إضافة نطاقات الشبكة المتأثرة إلى تكوين تجاوز الشبكة الداخلية. وهذا يسمح للنظام بالحفاظ على نسب هوية المستخدم للطلبات الناشئة من هذه الشبكات.

الخطوة 3: إختبار الوصول إلى التطبيق

بعد تنفيذ بديل IP، اختبر التطبيقات المتأثرة للتحقق من:

- يتم نسب طلبات موارد عبر المجال بشكل صحيح إلى هوية المستخدم
- تتم تهيئة التطبيقات بنجاح بدون أخطاء CORS
- تظهر سجلات الأنشطة هوية المستخدم بدلا من هوية الشبكة أو الهوية المستندة إلى النفق لجميع الطلبات

الخطوة 5: مراقبة تقارير الأنشطة

أستخدم مراقبة > بحث عن النشاط للتحقق من أن الطلبات قد تم الآن إسنادها بشكل صحيح إلى المستخدمين المصادق عليهم بدلا من إظهار هوية مستندة إلى شبكة أو نفق.

السبب

من المتوقع أن يحدث هذا السلوك بسبب طبيعة مصادقة SAML المقترنة بدائل Cookie في البيئات الافتراضية. عندما تقوم تطبيقات ويب بإجراء عمليات إعادة توجيه عبر المجال أو إحضار موارد من مجالات مرتبطة متعددة، من المحتمل أن لا تحمل الطلبات التي تمت إعادة توجيهها ملف تعريف الارتباط البديل بطريقة يمكن أن يقترن بها Cisco Secure Access مرة أخرى إلى جلسة عمل المستخدم التي تمت مصادقتها.

السبب الجذري يقع لأن:

- تعتمد "بدائل ملفات تعريف الارتباط" على نشر ملفات تعريف الارتباط للمستعرض عبر عمليات إعادة التوجيه.
- يمكن لسياسات الأمان عبر المجال (CORS) نزع ملفات تعريف الارتباط أثناء سيناريوهات 307/إعادة التوجيه.
- تمنع إجراءات أمان المستعرض مشاركة ملفات تعريف الارتباط عبر مجالات مختلفة.
- تتعامل بيئات سطح المكتب الظاهرية مع نشر ملفات تعريف الارتباط بشكل مختلف عن الأجهزة المادية.

بمجرد فقدان تعيين المستخدم إلى ملف تعريف الارتباط، يتعذر على Secure Access حل الطلب للمستخدم الذي تمت مصادقته، مما يتسبب في نسب الطلب فقط إلى الشبكة المسجلة/الهوية المختلفة كمصدر وتم حظره بعد ذلك بواسطة قواعد الرفض الافتراضية.

المحتوى ذي الصلة

- 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).