فشل المصادقة من خلال WSA عندما يستخدم العميل Negotiate

المحتويات

المقدمة

يوضح هذا المستند كيفية التحكم في المشكلة عند فشل المصادقة من خلال جهاز أمان الويب (WSA) من Cisco عندما يستخدم العميل المفاوضات.

معلومات أساسية

يمكن لجهاز أمان الويب (WSA) من Cisco مصادقة المستخدمين لتطبيق السياسات استنادا إلى المستخدم أو المجموعة. أحد الطرق المتاحة هي Kerberos. عند إستخدام Kerberos كطريقة مصادقة في هوية، يستجيب WSA لطلب HTTP الخاص بالعميل باستخدام إستجابة HTTP 401 (شفافة) أو 407 (صريحة) تحتوي على الرأس **WWW-Authenticate: تفاوض**. عند هذه النقطة، يرسل العميل طلب HTTP جديدا مع **التخويل:** رأس **التفاوض**، والذي يحتوي على واجهة برنامج تطبيق خدمة الأمان العامة (GSS-API) وبروتوكولات التفاوض المحمي البسيط (SPNEGO). تحت SPNEGO، يعرض المستخدم **أنواع الأجهزة** التي يدعمها. هذه هي أنواع الأجهزة التي تدعمها WSA:

- KRB5- طريقة مصادقة Kerberos التي يتم إستخدامها إذا تم دعم Kerberos وتكوينه بشكل صحيح على العميل وإذا كانت تذكرة Kerberos صالحة موجودة للخدمة التي يتم الوصول إليها
- NTLMSSP- أسلوب موفر دعم أمان Microsoft NTLM الذي يتم إستخدامه في حالة عدم توفر تذاكر Kerberos صالحة ولكن أسلوب مصادقة التفاوض معتمد

المشكلة: يفشل المصادقة من خلال WSA عندما يستخدم العميل NegotiateEXTS

في الإصدارات الأحدث من Microsoft Windows، يتم دعم أسلوب مصادقة جديد يسمى NegoExts، وهو ملحق لبروتوكول مصادقة Negotiate. يعتبر هذا النوع من الوسائط أكثر أمانا من NTLMSSP، ويفضل بواسطة العميل عندما تكون الأساليب الوحيدة المدعومة هي NEGOTIATEexts و NTLMSSP. يمكن العثور على مزيد من المعلومات في هذا الارتباط:

تقديم ملحقات لحزمة مصادقة Negotiate

يحدث هذا السيناريو عادة عندما يتم تحديد أسلوب مصادقة التفاوض ولا يوجد KRB5 mechType (غالبا بسبب فقدان تذكرة Kerberos صالحة لخدمة WSA). إذا اختار العميل NegotiateEXTS (يمكن اعتباره NEGOTIATEex في وضع Wireshark)، فلن يتم تعطيل WSA لمعالجة معاملة المصادقة وفشل المصادقة للعميل. عند حدوث ذلك، تظهر هذه السجلات في سجلات المصادقة:

```
Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP 14
   packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH :
      ........ 123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS
```

عند فشل المصادقة، يحدث هذا:

في حالة تمكين امتيازات الضيف - يتم تصنيف العميل على أنه **غير مصدق عليه** وإعادة توجيهه إلى موقع الويب

إذا تم تعطيل امتيازات الضيف - يتم تقديم العميل مع 401 أو 407 آخرين (وفقا لأسلوب الوكيل) مع طرق المصادقة المتبقية المعروضة في رأس الاستجابة (لا يتم تقديم التفاوض مرة أخرى). من المحتمل أن يتم حدوث مطالبة مصادقة إذا تم تكوين NTLMSSP و/أو المصادقة الأساسية. إذا لم يكن هناك طرق مصادقة أخرى (يتم تكوين الهوية فقط ل Kerberos)، ببساطة يفشل المصادقة.

الحل

يكمن الحل لهذه المشكلة في إزالة مصادقة Kerberos من الهوية - أو- إصلاح العميل حتى يحصل على تذكرة Kerberos صالحة لخدمة WSA.

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).