أستكشاف أخطاء الوصول إلى موقع SWG وإصلاحها لبوابة الويب الآمنة

المحتويات

المقدمة

يصف هذا المستند المنهجية المنظمة لتشخيص مشاكل الوصول إلى موقع الويب عند توجيهها من خلال وكيل مستند إلى مجموعة النظراء (عبارة الويب الآمنة/SWG)، ولكن ليس عند إستخدام الوصول المباشر إلى الإنترنت (DIA).

- النطاق: يطبق على كل من Cisco Secure Access و Cisco Umbrella SIG.

المتطلبات الأساسية والتخيرات المهمة

- تحقق من تنفيذ جميع عمليات أستكشاف الأخطاء وإصلاحها على المشاكل القابلة لإعادة الإنشاء.
- قم بتجميع ملف HAR (أرشيف HTTP) والتقاط حزمة متزامن (PCAP) لتوفير بيانات دقيقة للتحليل.
- قد تؤثر التغييرات على سياسات الوكيل (على سبيل المثال، تخطي فك التشفير أو الفحص) على وضعية الأمان؛ تطبيق فقط على أستكشاف الأخطاء وإصلاحها أو كما هو موصى به.

تحديد أخطاء مستوى الوكيل

تشمل مؤشرات التدخل الوكيل الشائعة ما يلي:

- عبارة 502 Bad
- شهادة 515 Upstream غير موثوق بها
- 517 تم إبطال شهادة تدفق البيانات
- 403 ممنوع
- الشهادات الملغاة
- عدم تطابق مجموعة التشفير
- مهلات اتصال موقع الويب

منهجية أستكشاف الأخطاء وإصلاحها

الخطوة 1: تأكيد حركة مرور البيانات التي تجتاز الوكيل

- جمع البيانات: قم بإنشاء ملف HAR و PCAP عند حدوث المشكلة.
- تحليل العنوان: فحص رأس VIA في استجابات HTTP. يؤكد وجود s_proxy (وكيل NGINX) أو m_proxy (خدمة الوكيل المنطقية/MPS) أن حركة مرور البيانات هي وكيل.
- تدفق TCP: في Wireshark، اتبع تدفق TCP لضمان الاتصال ب IP للوكيل، وليس IP للوجهة.

الخطوة 2: التحقق من حالة فك تشفير TLS

- فحص المستعرض: انقر أيقونة القفل في شريط عنوان المستعرض. إذا ظهرت شهادة جذر الوصول الآمن من Cisco في سلسلة الشهادات، يكون فحص HTTPS نشطا.
- التحقق من الصحة: مرجع تبادلي سوؤرل VIA في ملفات HAR/PCAP.
- أمر OpenSSL: لمعاينة سلاسل الشهادات:

```
openssl s_client -connect www.example.com:443 - ضورع
```

يتحقق هذا الأمر من سلسلة الشهادات المقدمة من قبل الخادم. قم بتشغيله من جهاز يجتاز الوكيل للتحقق المباشر.

الخطوة 3: العزل وعملية القضاء على الأسلحة النووية

1. المرحلة أ - إختبار فحص HTTPS (طبقة NGINX):
   - قم بإضافة المجال المثير للمشاكل إلى قائمة "دعم فك تشفير" SWG.
   - الحفاظ على تمكين فحص الملفات.
   - إذا تم حل المشكلة: من المحتمل أن يكون السبب الجذري فحص NGINX SSL/TLS. تحليل PCAP لعدم تطابق التشفير أو مشاكل SNI. أستخدم ملتقطات الفافة مع أو بدون وكيل لمقارنة السلوك.
   - إذا إستمرت المشكلة: انتقل إلى المرحلة B.
2. المرحلة ب - فحص الملف الاختباري (طبقة المسح الضوئي):
   - قم بتعطيل فحص الملف لحركة المرور المحددة.
   - إذا تم حل المشكلة: يكمن السبب الجذري في محرك مسح الملفات. راجع PCAP و HAR، قم بإعادة الإنتاج في المختبر، وحدد إذا ما كان نوع ملف معين أو توقيع يؤدي مسح ضوئي إلى تشغيل المشكلة.
   - إذا لم يتم الحل: اتصل بالدعم باستخدام السجلات ونتائج الملف.

المشكلات الشائعة ورموز الأخطاء

شهادة 515 Upstream غير موثوق بها

تتضمن الوجهة. شهادة مخادم من صحة قق التحقق SWG لكيلو على يتعذر عندما الخطأ هذا يحدث ملتمكة غير أو اياتذ عقموو أو ةيحالصلا ةيهتنم تاداهشلا لسالس بابسألا.

- الشهادة. في أخطاء توجد ال ؛الشبكي عقوملا لماعأ :في فلملا صحف + HTTPS صحف
- تقرير المستخدم. ،515 خطأ ةظحالم تمت :تافلملا صحف ليغشت فاقيإ + HTTPS صحف ليغشت
- ل. مشاكل أي ةظحالم متت مل :(ريفشتلا كف مدع ةمئاق على دوجوملا لاجملا) تافلملا صحف ليغشت فاقيإ + HTTPS صحف ليغشت فاقيإ

التفاصيل الفنية: دق يفشل وكيل NGINX إذا كان الخادم مداخ الخادم مداخ الخادم مداخ الخادم يعتمد على جلب الوصول إلى معلومات المرجع (AIA) للحصول على شهادات وسيطة مفقودة، حيث إن NGINX ال يتعامل مع AIA بسهولة مثل خدمة وكيل مسح الملفات. يمكن أن تؤدي عدم مطابقة SNI و SAN أثناء مصافحة TLS إلى حدوث حالات فشل أيضا.

517 تم إبطال شهادة تدفق البيانات

مداخ شهادة أن وجد وكيل SWG الخاص OCSP أو CRL من التحقق أن 517 أطخ يعني المنبع ملغية.

- استكشاف الأخطاء وإصلاحها: استخدم أدوات خارجية مثل SSL لمعامل أو OpenSSL لتأكيد حالة الإبطال.
- التوثيق:
  - [خطأ استكشاف الأخطاء وإصلاحها 517 من Cisco - تم إبطال شهادة البث]()
  - [فهم أخطاء البروتوكول والشهادة الشائعة]()

خيارات معالجة خطأ الشهادة

يقدم Cisco Secure Access ميزة جديدة تسمى "خيارات معالجة خطأ الشهادة" لتجاوز الأخطاء التي تؤدي إلى متعدد المستويات دون تعطيل فك التشفير بالكامل. يمكن إدارة المجالات التي تؤدي إلى أخطاء الشهادة بسبب الفحص باستخدام هذه الميزة بدلا من قوائم "عدم فك التشفير" الواسعة.
توجد هذه الميزة في Umbrella SIG اعتبارا من اليوم. تفاصيل طلبات الميزة ل CSA.

عبارة 502 Bad

يشير الخطأ 502 إلى أن وكيل SWG تلقى إستجابة غير صحيحة من خادم الخادم الخادم أثناء العمل كوسيط.

- تدفق البيانات: العميل إلى وكيل SWG
- للتحميل: وكيل SWG للخادم الوجهة

دائما ما يكون الخطأ في اتصال الباب- بسبب أخطاء في البروتوكول أو رسائل إعادة ضبط TCP أو رؤوس غير مكونة بشكل صحيح.

الأسباب الشائعة 502

- مجموعات تشفير SWG غير المدعومة
- طلب مصادقة شهادة العميل
- الرؤوس المضافة بواسطة وكيل SWG

مجموعات شفرة غير مدعومة

السبب: يتطلب الخادم تشفير غير مدعوم من قبل SWG (على سبيل المثال، TLS_CHACHA20_POLY1305_SHA256).
الدقة: إضافة المجال إلى قائمة فك التشفير الانتقائي.

أوامر الاختبار:
باستخدام الوكيل:

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k https://www.cnn.com" >> غراف
```

بدون وكيل:

```
curl -v www.xyz.com:80
```

نظام التشغيل Mac/Linux:

```
curl -vvv -o /dev/null -k -l www.cnn.com
```

Windows:

```
curl -vv -o null -k -l www.cnn.com
```

طلب مصادقة شهادة العميل

السبب: يتطلب خادم الخادم الخادم الخادم شهادات من جانب العميل، لا تعتمدها SWG.

الدقة: تجاوز المجال من الوكيل باستخدام قائمة إدارة المجالات الخارجية (Umbrella SIG) أو تجاوز الوكيل الآمن (Cisco Secure Access). تجاوز فحص HTTPS وحده غير كاف.

رؤوس تمت إضافتها بواسطة الوكيل

السبب: ترفض بعض الخوادم الطلبات التي تحتوي على رأس X-Forwarding-for (XFF) الذي تمت إضافته بواسطة SWG عند تمكين فحص HTTPS.
الدقة: قارن السلوك مع/بدون HTTPS و فحص الملف. إذا حدث الخطأ فقط عند وجود XFF، فمن المحتمل أن يكون خادم ويب تم تكوينه بشكل غير صحيح.

مثال:

curl https://www.xyz.com -k – رأس 'X-Forwarding-ل: 1.1.1.1' -o /dev/null -w "رمز الحالة: %{http_code}" -s

رمز الحالة: 502

curl https://www.xyz.com -k -o /dev/null -w رمز الحالة: %{http_code}" -s

رمز الحالة: 200

تتم إضافة رأس XFF للموقع الجغرافي. إذا تعذر على الخادم معالجتها، فسينتج خطأ 502.

من المحتمل أن تكون ملفات PUA أو ملفات تالفة غير مرغوب فيها

إذا لم تتمكن SWG من مسح ملف باستخدام التفتيش على الملف (على سبيل المثال، لتمكين الملفات المحمية، أو ملفات النطاق المطلوبة، أو ملفات تالفة)، فإنها تمنع التنزيل (ملف محمي) والتقارير - محظورة - من المحتمل أن يكون تطبيق غير مرغوب فيه

- أستكشاف الأخطاء وإصلاحها: التقاط HAR أثناء حدث الحظر. إستخدام Override Security كحل بديل مؤقت. إذا كان الملف تالفا أو ضارا، فيجب تصحيحه في المصدر.

الفئات التي يحتمل أن تكون ضارة ومجموعات السمعة

- أستخدم Talos للتحقق من سمعة الويب (WBRS). إذا تم تصنيف مجال بشكل خاطئ، ولكن Talos يعتقد أنه آمن، فقم بتقديم طلب COG JIRA إلى Talos للمراجعة. إذا كنت بحاجة إلى فحص من خدمة Beaker من SWG، فقم بإزالة SWG

تم رفض الوصول من قبل Akamai لعناوين IP الخاصة بمخرج SWG

- يستخدم SWG عناوين IP للمخرج المشترك. إذا تم إدراج هذه العناصر على القائمة السوداء بواسطة خدمات سمعة IP (على سبيل المثال، RapidCloud)، فقد يتم رفض الوصول إلى مواقع معينة.

المشكلات الشائعة: [لا يتوفر منفذ تسجيل الدخول YouTube Sign-In والفيديو]

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).