تجنب ضعف الكلب والبدل عند إستخدام ASA و AnyConnect

المحتويات

المقدمة

يصف هذا المستند ما يجب عليك فعله لتجنب إضافة Oracle على قابلية قابلية التشفير القديمة (PODLE) المنخفضة عند إستخدام أجهزة الأمان المعدلة (ASAs) و AnyConnect لاتصال طبقة آخذ التوصيل الآمنة (SSL).

معلومات أساسية

يؤثر قابلية الوصول إلى نقطة الوصول على بعض عمليات التنفيذ لبروتوكول إصدار أمان طبقة النقل 1 (TLSv1) وقد يسمح للمهاجم البعيد غير المصدق عليه بالوصول إلى المعلومات الحساسة.

يرجع الضعف إلى وضع تشفير الكتلة غير الصحيح المنفذ في TLSv1 عند إستخدام وضع توصيل كتلة التشفير (CBC). ويمكن للمهاجم أن يستغل نقاط الضعف لتنفيذ هجوم بالقناة الجانبية على الرسالة المشفرة. وقد يسمح إستغلال ناجح للمهاجم بالوصول إلى معلومات حساسة.

المشكلة

يسمح ASA بتوصيلات SSL الواردة في نموذجين:

1. WebVPN بدون عملاء
2. عميل AnyConnect

ومع ذلك، لا تتأثر أي من عمليات تنفيذ TLS على ASA أو عميل AnyConnect بمؤشر PODLE. وبدلا من ذلك، يتأثر تنفيذ SSLv3 حتى يكون أي عملاء (متصفح أو AnyConnect) يتفاوضون SSLv3 عرضة لهذا الضعف.

> **تحذير**: لا تؤثر عضات نقطة الوصول على TLSv1 على ASA. لمزيد من المعلومات حول المنتجات والإصلاحات المتأثرة، ارجع إلى CVE-2014-8730.

الحل

طبقت Cisco هذه الحلول لهذه المشكلة:

1. تم إهمال جميع إصدارات AnyConnect التي كانت مدعومة (تم التفاوض عليها) لـ اقباس ل SSLv3، ولن تتفاوض الإصدارات المتوفرة للتنزيل (كلا v3.1x و v4.0) مع SSLv3 حتى لا تكون عرضة للإصدار.

2. تم تغيير إعداد البروتوكول الافتراضي لـ ASA من SSLv3 إلى TLSv1.0 بحيث يكون الاتصال الوارد من عميل يدعم TLS، وهذا ما سيتم التفاوض بشأنه.

3. يمكن تكوين ASA يدويا لقبول بروتوكولات SSL المحددة فقط باستخدام هذا الأمر:

   [ssl server-version](#)

   كما هو مذكور في الحل 1، لا يوفر أي من عملاء AnyConnect المدعومة حاليا بالتفاوض على SSLv3 بعد الآن، وبالتالي سيفشل العميل في الاتصال بأي ASA تم تكوينه باستخدام أي من هذه الأوامر:

   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   ومع ذلك، بالنسبة لعمليات النشر التي تستخدم إصدارات v3.0.x و v3.1.x AnyConnect التي تم إهمالها (والتي هي جميع إصدارات بنية AnyConnect pre 3.1.05182)، والتي يتم فيها إستخدام تفاوض SSLv3 بشكل محدد، فإن الحل الوحيد هو القضاء على إستخدام SSLv3 أو النظر في ترقية العميل.

4. سيتم دمج الإصلاح الفعلي لوحدات تب (معرف تصحيح الأخطاء من Cisco [CSCus08101](#)) في أحدث إصدارات الإصدار المؤقتة فقط. يمكنك الترقية إلى إصدار ASA يحتوي على الإصلاح لحل المشكلة. أول إصدار متوفر على Cisco Connection Online (CCO) هو الإصدار 9.3(2.2).

   تكون الإصدارات الأولى من برنامج ASA الثابت لهذا الضعف كما يلي:
   8-2 القطار: 8-2-5-558-4 القطار: 8-4-7-269،0 القطار: 9،0،4،299-1 القطار: 9-1-69-2 القطار: 9-2-3-39-3 القطار: 9-3-2-2

TLSv1.2

- يدعم ASA TLSv1.2 كإصدار برنامج 9.3(2).
- يدعم عملاء AnyConnect الإصدار 4.x جميع عملاء TLSv1.2.

وهذا يعني:

- إذا كنت تستخدم WebVPN بدون عميل، فيمكن لأي ASA الذي يشغل هذا الإصدار من البرنامج أو إصدار أعلى التفاوض على TLSv1.2.

- إذا كنت تستخدم عميل AnyConnect، لاستخدام TLSv1.2، فستحتاج إلى الترقية إلى عملاء الإصدار 4.x.

معلومات ذات صلة

- الطراز CVE-2014-8730
- معرف تصحيح الأخطاء من Cisco CSCug51375
- Cisco Bug ID CSCur42776

- الدعم التقني والمستندات - Cisco Systems

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).