حلول مكامن الضعف ل ASA BEAST

المحتويات

المقدمة

يصف هذا المستند الثغرات الأمنية داخل برنامج أجهزة الأمان المعدلة (ASA) من Cisco الذي يسمح للمستخدمين غير المصرح لهم بالوصول إلى المحتوى المحمي. يتم وصف الحلول البديلة لهذه المشكلة أيضا.

المشكلة

تتم الاستفادة من ميزة المستعرض التي تستغل ضد قابلية SSL/TLS (BEAST) بواسطة المهاجم لقراءة المحتوى المحمي بشكل فعال عبر سلاسل متجهات التهيئة (IV) في وضع تشفير مجموعات التشفير (CBC) باستخدام هجوم نص عادي معروف.

يستخدم الهجوم أداة تستغل حالة الضعف في بروتوكول TLSv1 (Transport Layer Security Version 1) المستخدم على نطاق واسع. والمسألة ليست متجذرة في البروتوكول نفسه، بل هي عبارة عن مجموعة شفرة من المواد التي يستخدمها. يدعم TLSv1 والإصدار 3 من طبقة مآخذ التوصيل الآمنة (SSLv3) شفرات CBC، حيث يحدث هجوم Oracle المحشو.

تأثير المستخدم

وكما يشير إستطلاع تنفيذ SSL SSL Pulse، الذي تم إنشاؤه بواسطة حركة إنترنت جديرة بالثقة، فإن أكثر من 75٪ من خوادم SSL عرضة لهذا الضعف. ومع ذلك، فإن الأمور اللوجستية المتعلقة بأداة BEAST معقدة إلى حد ما. لاستخدام BEAST للتنصت على حركة المرور، يجب أن يكون للمهاجم القدرة على قراءة الحزم وضخها بسرعة كبيرة. ومن المحتمل أن يحد هذا من الأهداف الفعالة لهجوم الوحش. فعلى سبيل المثال، يستطيع المهاجم BEAST انتزاع حركة مرور عشوائية بشكل فعال في نقطة ساخنة لشبكة WiFi أو حيث يتم اعتراض حركة مرور الإنترنت بالكامل من خلال عدد محدود من بوابات الشبكة.

الحل

الوحش هو إستغلال للضعف في الشفرة الذي يستخدمه البروتوكول. بما أنه يؤثر على تشفير CBC، فإن الحل البديل الأصلي لهذه المشكلة كان الانتقال إلى تشفير RC4 بدلا من ذلك. ومع ذلك، تكشف نقاط الضعف في خوارزمية الجدولة الرئيسية لمقال RC4 الذي نشر في عام 2013 أنه حتى RC4 كان لديه ضعف جعله غير مناسب.

in order to عالجت هذا إصدار، cisco طبقت هذا إثنان إصلاح ل ال ASA:

- معرف تصحيح الأخطاء من CSCts83720 Cisco: *الترقية إلى TLS 1.1/1.2*

ترقية واستخدام TLS 1.1/1.2. التحديد مع هذا الحل هو أنه يطبق فقط على ASA 5500-X ASA منصة. لا تدعم أجهزة التشفير على أنظمة ASA الأساسية القديمة (ASA 5505 و TLSv1.2 (ASA 5500 series. ونتيجة لهذا فإن إصلاح هذه المنصات أمر غير ممكن.

نظرا لقيود البروتوكول، لا يوجد حل ل SSLv3 أو TLSv1.0؛ ومع ذلك، قامت معظم المستعرضات الحديثة بتنفيذ طرق مختلفة للتخفيف.

- معرف تصحيح الأخطاء من Cisco CSCuc85781: *WebVPN Cookie Randomization*

بالنسبة لإصدارات برنامج ASA التي لا تدعم TLSv1.2، جعلت Cisco ملفات تعريف الارتباط عشوائية مع هذا الإصلاح لتقليل المخاطر. وهذا لا يمنع هجمات الحيوانات تماما، ولكنه يساعد في التخفيف منها.

تلميح: الطريقة الوحيدة للحماية الكاملة من التعرض للوحش هي إستخدام TLSv1.2. هذا مشابه للشفرات. تستمر Cisco في إضافة شفرات أحدث وأقوى في التعليمات البرمجية الأحدث، وقد تواجه الشفرات الأقدم مشاكل معروفة (مثل RC4). لذلك، توصي Cisco بالانتقال إلى البروتوكولات والشفرات الأحدث.

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).