نقطة الضعف في وضع CBC لبروتوكول SSL v3 و TLS v1

المحتويات

المقدمة

يصف هذا وثيقة كيف أن وضع تشفير كتلة التشفير (CBC) أسلوب تشفير على الـ cisco بريد الإلكتروني أمن تطبيق (ESA). قد يشير تدقيق/مسح الأمان إلى أن ESA يحتوي على طبقة آخذ التوصيل الآمنة (SSL) v3/أمان طبقة النقل (TLS) v1 بروتوكول الثغرات الضعيفة في وضع CBC.

> **Attention**: إذا كنت تقوم بتشغيل التعليمات البرمجية القديمة لـ AsyncOS لأمان البريد الإلكتروني، فمن المستحسن الترقية إلى الإصدار 11.0.3 أو الإصدار الأحدث. يرجى مراجعة ملاحظات إصدار أمان البريد الإلكتروني من Cisco للحصول على أحدث الإصدارات والمعلومات الخاصة بنا. إذا كنت بحاجة إلى مزيد من المساعدة بشأن الترقيات أو تعطيل التشفير، فيرجى فتح حالة دعم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى AsyncOS لأمان البريد الإلكتروني (أي مراجعة)، و Cisco ESA، و ESA ظاهري.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

- يتطلب التوافق مع معيار أمان بيانات صناعة بطاقة الدفع (PCI DSS) تعطيل تشفير CBC.
- قام تدقيق/مسح الأمان بتحديد نقطة ضعف محتملة مع بروتوكولات SSL v3/TLS v1 التي تستخدم شفرات وضع CBC.

  تلميح: الإصدار 3.0 من SSL (RFC-6101) هو بروتوكول قديم وغير آمن. هناك قابلية للتأثر في SSLv3 CVE-2014-3566 المعروفة باسم إضافة Oracle على وجوه التشفير القديم (PODLE) المخفض، Cisco Bug id CSCur27131. تتمثل التوصية في تعطيل SSL v3 أثناء تغيير المشفرات واستخدام TLS فقط وتحديد الخيار 3 (TLS v1). راجع معرف تصحيح الأخطاء CSCur27131 المتوفر من Cisco للحصول على تفاصيل كاملة.

يتم إستخدام بروتوكولات SSL v3 و TLS v1 من أجل توفير التكامل والأصالة والخصوصية للبروتوكولات الأخرى مثل HTTP وبروتوكول الوصول إلى الدليل خفيف الوزن (LDAP). وهي توفر هذه الخدمات باستخدام التشفير للخصوصية، وشهادات x509 للأصالة، ووظائف التشفير أحادي الإتجاه للسلامة. لتشفير البيانات، يمكن لـ SSL و TLS إستخدام تشفير الكتلة الذي وهو خوارزميات تشفير يمكنها تشفير كتلة ثابتة فقط من البيانات الأصلية إلى كتلة مشفرة بنفس الحجم. لاحظ أن تلك الشفرات ستحصل دائما على نفس الكتلة الناتجة لنفس الكتلة الأصلية للبيانات. لتحقيق فرق في الإنتاج، الإنتاج من التشفير وهو XORed مع كتلة أخرى من نفس الحجم يشار إليه باسم متجهات التهيئة (IV). تستخدم CBC ربما واحدا للكتلة الأولية ونتيجة الكتلة السابقة لكل كتلة تالية للحصول على الفرق في مخرجات تشفير الكتلة المشفرة.

في تطبيق SSL v3 و TLS v1، كان إستخدام وضع CBC المختار ضعيفا لأن حركة المرور بأكملها تشارك جلسة CBC واحدة من مجموعة واحدة من عناوين IV الأولية. أما بقية الوحدات الوصفية، كما ذكر سابقا، فهي تتألف لتشفير الوحدات السابقة. الرباعيات التالية متاحة للقائمين على التنصت. وهذا يسمح للمهاجم الذي لديه إمكانية ضخ حركة مرور عشوائية إلى تدفق النص العادي (الذي يتم تشفيره بواسطة العميل) للتحقق من تخمينه للنص العادي الذي يسبق الكتلة التي تم حقنها. إذا كان تخمين المهاجمين صحيح، فعندئذ يكون إخراج التشفير هو نفسه لجمعتين.

بالنسبة للبيانات المنخفضة الإنتروبيا، من الممكن تخمين كتلة النص العادي بعدد قليل نسبيا من المحاولات. على سبيل المثال، للبيانات التي لها 1000 إمكانية، يمكن أن يكون عدد المحاولات 500.

المتطلبات

وهناك العديد من المتطلبات التي لابد من تلبيتها حتى يعمل الاستغلال:

1. يجب أن يستخدم اتصال SSL/TLS أحد شفرة تشفير الكتلة التي تستخدم أوضاع CBC، مثل DES أو AES. الـ تخضع القنوات التي تستخدم شفرات الدفق مثل RC4 للعيب. تستخدم نسبة كبيرة من إتصالات SSL/TLS RC4.
2. لا يمكن إستغلال الثغرات إلا من قبل شخص يعترض البيانات على اتصال SSL/TLS، كما يرسل بنشاط بيانات جديدة على هذا الاتصال. يتسبب إستغلال هذا الخلل في إنهاء اتصال SSL/TLS. يجب أن يواصل المهاجم مراقبة الاتصالات الجديدة واستخدامها حتى يتم تجميع بيانات كافية لفك تشفير الرسالة.
3. بما أن الاتصال يتم إنهاؤه في كل مرة، فيجب أن يكون عميل SSL/TLS قادرا على الاستمرار في إعادة إنشاء قناة SSL/TLS لفترة طويلة تكفي لفك تشفير الرسالة.
4. يجب أن يقوم التطبيق بإعادة إرسال نفس البيانات على كل اتصال SSL/TLS يقوم بإنشائه ويجب أن يتمكن المستمع من تحديد موقعه في تدفق البيانات. بروتوكولات مثل IMAP/SSL التي تحتوي على مجموعة ثابتة من الرسائل لتسجيل

الدخول للوفاء بهذا المتطلب. إستعراض الويب العام غير صحيح.

تهديد

نقطة ضعف CBC هي TLS v1. وقد لظ هذا الضعف قائما منذ أوائل عام 2004 وتم حله في الإصدارات اللاحقة من نظام TLS V1.1 و TLS v1.2.

قبل AsyncOS 9.6 لأمان البريد الإلكتروني، تستخدم ESA شفرات وضع TLS v1.0 و CBC. مع إصدار AsyncOS 9.6، يقدم ESA TLS v1.2. ومع ذلك، يمكن تعطيل شفرة وضع CBC، ويمكن إستخدام شفرة RC4 فقط، والتي ال تخضع للعيب.

بالإضافة إلى ذلك، في حالة تمكين SSLv2، قد يؤدي ذلك إلى تشغيل نتيجة إيجابية خاطئة لهذا الضعف. من المهم للغاية تعطيل SSL v2.

الحل

Attention: إذا كنت تقوم بتشغيل التعليمات البرمجية القديمة ل AsyncOS لأمان البريد الإلكتروني، فمن المستحسن الترقية إلى الإصدار 11.0.3 أو الإصدار الأحدث. يرجى مراجعة ملاحظات إصدار أمان البريد الإلكتروني من Cisco للحصول على أحدث الإصدارات والمعلومات الخاصة بنا. إذا كنت بحاجة إلى مزيد من المساعدة بشأن الترقيات أو تعطيل التشفير، فيرجى فتح حالة دعم.

قم بتعطيل شفرات وضع CBC لترك شفرات RC4 الممكنة فقط. ثبتت الأداة أن يستعمل TLS v1 فقط، أو TLS v1/TLS v1.2:

1. سجل الدخول إلى واجهة سطر الأوامر.
2. أدخل الأمر **sslconfig**.
3. دخلت الأمر **gui**.
4. أختر الخيار رقم 3 ل "TLS v1" أو كما هو مدرج في AsyncOS 9.6 "TLS v1/TLS v1.2".
5. أدخل هذه الشفرة:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. دخلت الأمر: **داخل**.
7. أختر الخيار رقم 3 ل "TLS v1" أو كما هو مدرج في AsyncOS 9.6 "TLS v1/TLS v1.2".
8. أدخل هذه الشفرة:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. أدخل الأمر **الصادر**.
10. أختر الخيار رقم 3 ل "TLS v1" أو كما هو مدرج في AsyncOS 9.6 "TLS v1/TLS v1.2".
11. أدخل هذه الشفرة:
    `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. اضغط على **Enter** حتى تعود إلى موجه أمر اسم المضيف.
13. أدخل الأمر **commit**.
14. إنهاء الالتزام بالتغييرات.

تم تكوين ESA الآن لدعم TLS v1 أو TLSv1/TLS v1.2 فقط باستخدام شفرات RC4 أثناء عدم السماح بأي عوامل تصفية CBC.

فيما يلي قائمة التشفير المستخدمة عند تعيين RC4:-SSLv2. لاحظ أنه ال توجد شفرات

وضع CBC في القائمة.

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

وفي حين أن هذا الاستغلال لا يثير قلقا كبيرا بسبب تعقيده ومتطلبات إستغلاله، فإن أداء هذه الخطوات يشكل ضمانة كبيرة لمنع أي أعمال مستغلة محتملة، فضلا عن تمرير مسوحات أمنية صارمة.

معلومات ذات صلة

- [جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي]
- [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).