إصلاح خطأ خوارزميات التشفير AnyConnect مع تمكين FIPS

المحتويات

المقدمة

يوضح هذا المستند لماذا قد لا يتمكن المستخدمون من الاتصال باستخدام عميل دعم معيار معالجة المعلومات الفيدرالية (FIPS) بجهاز أمان قابل للتكيف (ASA)، والذي يحتوي على سياسة تدعم خوارزميات التشفير التي تم تمكين FIPS بها.

معلومات أساسية

أثناء إعداد اتصال Internet Key Exchange الإصدار 2 (IKEv2)، لا يكون البادئ على علم بأي الاقتراحات مقبولة من قبل النظير، لذلك يجب على البادئ أن يخمن أي مجموعة Diffie-Hellman (DH) يتم إستخدامها عند إرسال رسالة IKE الأولى. مجموعة DH المستخدمة لهذا التخمين هي عادة أول مجموعة DH في قائمة مجموعات DH التي تم تكوينها. ثم يقوم البادئ بحساب البيانات الأساسية للمجموعات التي تم تخمينها ولكنه يرسل أيضا قائمة كاملة بكافة المجموعات إلى النظير، مما يسمح للنظير بتحديد مجموعة DH مختلفة إذا كانت المجموعة التي تم تخمينها خاطئة.

في حالة أي عميل، لا توجد قائمة مكونة من قبل المستخدم لنهج IKE. وبدلا من ذلك، هناك قائمة مسبقة التكوين من السياسات التي يدعمها العميل. ولهذا السبب، فمن أجل تقليل الحمل الحسابي على العميل عند حساب البيانات الأساسية للرسالة الأولى مع مجموعة قد تكون الرسالة غير صحيحة، تم طلب قائمة مجموعات DH من الأضعف إلى الأقوى. وبالتالي، يختار العميل أقل مجموعة DH كفاءة من حيث إستخدام الكمبيوتر، وبالتالي أقل مجموعة تستخدم الموارد بكفاءة للتخمين الأولي، ولكنه بعد ذلك ينتقل إلى المجموعة التي يختارها الاستقبال والبث في الرسائل التالية.

> **ملاحظة**: يختلف هذا السلوك عن عملاء AnyConnect الإصدار 3.0 الذين أمروا مجموعات DH من الأقوى إلى الأضعف.

ومع ذلك، في وحدة الاستقبال والبث، تكون المجموعة الأولى من مجموعة DH في القائمة هي المجموعة التي يرسلها العميل والتي تطابق مجموعة DH التي تم تكوينها على البوابة والتي تم تحديدها. وبالتالي، إذا كان لدى ASA أيضا مجموعات DH أضعف يتم تكوينها، فإنه يستخدم مجموعة DH الأضعف التي يتم دعمها من قبل العميل وتكوينها على وحدة الاستقبال والبث على الرغم من توفر مجموعة DH أكثر أمانا على كل الطرفين.

تم إصلاح هذا السلوك على العميل من خلال معرفة تصحيح الأخطاء من Cisco CSCub92935. تقوم جميع إصدارات العملاء التي تحتوي على الإصلاح من هذا الخطأ بعكس الترتيب الذي يتم به سرد مجموعات DH عند إرسالها إلى وحدة الاستقبال والبث. ومع ذلك، لتجنب حدوث

مشكلة توافق مع الإصدارات السابقة من البوابات غير Suite B، ظل مجموعة DH الأضعف (واحدة غير وضع FIPS واثنتان لوضع FIPS) في أعلى القائمة.

ملاحظة: بعد الإدخال الأول في القائمة (المجموعة 1 أو 2)، يتم إدراج المجموعات من حيث الأقوى إلى الأضعف. وهذا يضع مجموعات المنحنى البيضاوي أولا (21، 20، 19)، ثم مجموعات الأسية النمطية (MODP) (24، 14، 5، 2).

تلميح: إذا تم تكوين البوابة باستخدام مجموعات DH متعددة في نفس النهج، فيتم تضمين المجموعة 1 (أو 2 في وضع FIPS)، فسيقبل ASA المجموعة الأضعف. يتم تضمين الإصلاح فقط مجموعة DH 1 وحدها في سياسة تم تكوينها على البوابة. عند تضمين المجموعة 1، يتم ولكن لا يتم تضمين مجموعات متعددة في سياسة واحدة، تكوين تحديد الأقوى. على سبيل المثال:

- في الإصدار 9.0 من ASA (المجموعة B) مع تعيين سياسة IKEv2 على 1 2 5 14 24 19 20 21، **يتم تحديد المجموعة 1** كما هو متوقع.

- في الإصدار 9.0 من ASA (المجموعة B) مع تعيين سياسة IKEv2 على 2 5 14 24 19 20 21، **يتم تحديد المجموعة 21** كما هو متوقع.

- مع وجود العميل في وضع FIPS على الإصدار 9.0 من ASA (المجموعة B) مع تعيين نهج IKEv2 على 1 2 5 14 24 19 20 21، **يتم تحديد المجموعة 2** كما هو متوقع.

- مع وجود العميل الذي تم إختباره في وضع FIPS على الإصدار 9.0 من ASA (المجموعة B) مع تعيين نهج IKEv2 على 5 14 24 19 20 21، **يتم إختيار المجموعة 21** كما هو متوقع.

- في الإصدار 8.4.4 من ASA (غير المجموعة B) مع تعيين سياسة IKEv2 على 1 2 5 14، **يتم تحديد المجموعة 1** كما هو متوقع.

- في الإصدار 8.4.4 من ASA (غير المجموعة B) مع تعيين سياسة IKEv2 على 2 5 14، **يتم تحديد المجموعة 14** كما هو متوقع.

المشكلة

يتم تكوين ASA باستخدام سياسات IKEv2 التالية:

```
crypto ikev2 policy 1
encryption aes-gcm-256
integrity null
group 20
prf sha384 sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption aes-192
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 20
encryption aes
integrity sha
group 5 2
prf sha
```

```
lifetime seconds 86400
```

في هذا التكوين، يتم تكوين النهج 1 بشكل واضح لدعم جميع خوارزميات التشفير التي تم تمكين FIPS بها. ومع ذلك، عندما يحاول مستخدم الاتصال من عميل يدعم FIPS، يفشل الاتصال برسالة الخطأ:

```
The cryptographic algorithms required by the secure gateway do not match those supported by
AnyConnect.
Please contact your network administrator.
```

ومع ذلك، إذا قام المسؤول بتغيير النهج 1 بحيث يستخدم مجموعة DH 2 بدلا من 20، يعمل الاتصال.

الحل

واستنادا إلى الأعراض، فإن الاستنتاج الأول هو أن العميل يدعم مجموعة DH رقم 2 فقط عند تمكين FIPS والعميل أي من الآخرين. هذا في الواقع غير صحيح. إذا قمت بتمكين تصحيح الأخطاء هذا على ASA، فيمكنك رؤية الاقتراحات التي يرسلها العميل:

```
debug crypto ikev2 proto 127
```

أثناء محاولة الاتصال، تكون رسالة تصحيح الأخطاء الأولى:

```
IKEv2-PROTO-2: Received Packet [From 192.168.30.5:51896/To 192.168.30.2:500/
VRF i0:f0]
Initiator SPI : 74572B8D1BEC5873 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUESTIKEv2-PROTO-3: Next payload: SA, version:
2.0 Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 747
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 316
last proposal: 0x2, reserved: 0x0, length: 140
Proposal: 1, Protocol id: IKE, SPI size: 0, #trans: 15 last transform: 0x3,
reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-GCM
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-GCM
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-GCM
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: None
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_521_ECP/Group 21
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_384_ECP/Group 20
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_256_ECP/Group 19
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP_256_PRIME/Group 24
```

```
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP/Group 14
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5
last proposal: 0x0, reserved: 0x0, length: 172
Proposal: 2, Protocol id: IKE, SPI size: 0, #trans: 19 last transform: 0x3,
reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 12
type: 1, reserved: 0x0, id: AES-CBC
last transform: 0x3, reserved: 0x0: length: 8
type: 1, reserved: 0x0, id: 3DES
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 2, reserved: 0x0, id: SHA1
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA512
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA384
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA256
last transform: 0x3, reserved: 0x0: length: 8
type: 3, reserved: 0x0, id: SHA96
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1024_MODP/Group 2
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_521_ECP/Group 21
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_384_ECP/Group 20
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_256_ECP/Group 19
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP_256_PRIME/Group 24
last transform: 0x3, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_2048_MODP/Group 14
last transform: 0x0, reserved: 0x0: length: 8
type: 4, reserved: 0x0, id: DH_GROUP_1536_MODP/Group 5
KE Next payload: N, reserved: 0x0, length: 136
DH group: 2, Reserved: 0x0

fc c9 90 2b 15 35 31 34 0e 75 88 c0 f9 2a 1e 0a
a5 6b e3 8e e1 73 b9 d1 56 1e 60 9f 82 71 6c 4e
5c 1c a4 bd b5 23 a2 bc 82 f2 11 17 61 28 33 3f
02 c9 e7 cb f7 84 a6 22 4a 64 eb fa d7 84 a1 d9
ad c7 5d 77 cd 2a 65 79 95 9a d4 5c 22 8c 62 ae
0e fc c8 fd bd c8 4d 66 0d c3 69 d3 c4 cb e8 33
72 1a f1 cc 31 5f 08 75 65 6b 77 3b 23 c3 b8 74
02 fa 15 6e e4 7a b2 73 17 8f 08 02 20 7e b8 d7
N Next payload: VID, reserved: 0x0, length: 24

87 4d 63 76 cc 10 30 0e 4c 95 40 24 d3 b3 3b f3
44 be 0f e5
```

لذلك، وعلى الرغم من أن العميل قد أرسل المجموعات 2،21،20،19،24،14 و 5 (هذه المجموعات المتوافقة مع FIPS)، إلا أن الخادم لا يزال يتصل فقط بالمجموعة 2 التي تم تمكينها في النهج 1 في التكوين السابق. تصحح هذه المشكلة وأضحة أكثر في تصحيح الأخطاء:

```
IKEv2 received all requested SPIs from CTM to respond to a tunnel request.
IKEv2-PROTO-5: (64): SM Trace-> SA: I_SPI=74572B8D1BEC5873 R_SPI=E4160C492A824B5F
(R) MsgID = 00000006 CurState: R_VERIFY_AUTH Event: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: (64): Processing IKE_AUTH message
IKEv2-PROTO-1: Tunnel Rejected: Selected IKEv2 encryption algorithm (AES-CBC-192)
is not strong enough to secure proposed IPsec encryption algorithm (AES-GCM-256).
IKEv2-PROTO-1: (64): Failed to find a matching policy
IKEv2-PROTO-1: (64): Received Policies:
ESP: Proposal 1: AES-GCM-256 AES-GCM-192 AES-GCM-128 None Don't use ESN

ESP: Proposal 2: AES-CBC-256 AES-CBC-192 AES-CBC-128 3DES SHA512 SHA384 SHA256 SHA96
Don't use ESN

IKEv2-PROTO-1: (64): Failed to find a matching policy
IKEv2-PROTO-1: (64): Expected Policies:
ESP: Proposal 0: AES-GCM-256 SHA384 Don't use ESN

IKEv2-PROTO-5: (64): Failed to verify the proposed policies
IKEv2-PROTO-1: (64): Failed to find a matching policy
```

يفشل التوصيل بسبب مجموعة من العوامل:

1. عم تمكين FIPS، يرسل العميل سياسات محددة فقط ويجب أن تتطابق تلك السياسات. من بين هذه السياسات، فإنه يقترح فقط تشفير معيار التشفير المتقدم (AES) بحجم مفتاح أكبر من أو يساوي 256.

2. تم تكوين ASA باستخدام سياسات IKEv2 متعددة، إثنان منها تم تمكين المجموعة 2. كما هو موضح مسبقا، في هذا السيناريو، يتم إستخدام هذا النهج الذي يتضمن تمكين المجموعة 2 للاتصال. ومع ذلك، فإن خوارزمية التشفير في كل النهجين تستخدم حجم مفتاح 192، وهو منخفض جدا لعميل تم تمكين FIPS عليه.

لذلك، في هذه الحالة، يتصرف ASA والعميل وفقا للتكوين. هناك ثلاث طرق لحل هذه المشكلة لعملاء FIPS الذين تم تمكينهم:

1. قم بتكوين نهج واحد فقط باستخدام الاقتراحات الدقيقة المطلوبة.

2. إذا كانت هناك حاجة إلى عدة اقتراحات، فلا تقم بتكوين واحدة باستخدام المجموعة 2، وإلا فسيتم تحديد واحدة دائما.

3. إذا كان يجب تمكين المجموعة 2، فتأكد من أنها تحتوي على خوارزمية التشفير الصحيحة المكونة (AES-GCM-256 أو AES-256).

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).