توصيات ضد هجمات رش كلمة المرور الموجهة إلى خدمات VPN للوصول عن بعد في جدار الحماية الآمن

المحتويات

المقدمة

يصف هذا المستند التوصيات التي يجب أخذها في الاعتبار ضد هجمات رش كلمة المرور الموجهة إلى خدمات VPN للوصول عن بعد في جدار الحماية الآمن.

معلومات أساسية

هجمات رشاشات كلمات المرور هي نوع من هجوم القوة الغاشمة حيث يحاول المهاجم الوصول غير المصرح به إلى حسابات مستخدمين متعددين عن طريق المحاولة المنتظمة لعدد قليل من كلمات المرور المستخدمة بشكل شائع عبر العديد من الحسابات. يمكن أن تؤدي الهجمات الناجحة على رش كلمة المرور إلى الوصول غير المصرح به إلى المعلومات الحساسة واختراقات البيانات والحلول التوفيقية المحتملة لسلامة الشبكة

علاوة على ذلك، يمكن لهذه الهجمات، حتى في حالة فشلها في محاولة الوصول، إستهلاك موارد حسابية من جدار الحماية الآمن ومنع المستخدمين الصحيحين من الاتصال بخدمات VPN للوصول عن بعد.

التصرفات التي تتم ملاحظتها

عندما يتم إستهداف جدار الحماية الآمن لديك بواسطة هجمات رش كلمة المرور في خدمات VPN للوصول عن بعد، يمكنك تحديد هذه الهجمات من خلال مراقبة syslog واستخدام أوامر show معينة. وتتضمن أكثر السلوكيات شيوعا للبحث عنها ما يلي:

مبلغ غير عادي لطلبات المصادقة المرفوضة

تظهر وحدة الاستقبال والبث الخاصة بشبكة VPN Cisco Secure Firewall ASA أو FTD أعراض هجمات رش كلمة المرور بمعدل غير معتاد (100 ألف أو مليون) لمحاولات المصادقة المرفوضة.

ملاحظة: يمكن توجيه هذه المحاولات غير العادية للمصادقة إما إلى قاعدة البيانات المحلية أو إلى خوادم المصادقة الخارجية.

أفضل طريقة لاكتشاف هذا من خلال النظر إلى syslog. ابحث عن رقم غير عادي من أي من معرفات ASA syslog التالية:

- ٪ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database :

user

= *admin* : user

IP

= *x.x.x.x*

- ٪ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

- ٪ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.

اسم المستخدم مخفي دائما حتى يتم تكوين الأمر no logging hide username على ASA.

ملاحظة: هذا يعطي فكرة عن التحقق من إنشاء المستخدمين الصحيحين أو معرفتهم عن طريق الإساءة إلى عناوين IP، الرجاء توخي الحذر حيث أن أسماء المستخدمين ستكون مرئية في السجلات.

للتحقق، قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) ASA أو FTD، ثم قم بتشغيل الأمر show aaa-server ، وتحقق من وجود عدد غير عادي من طلبات المصادقة التي تم المحاولة عليها أو رفضها إلى أي من خوادم AAA التي تم تكوينها:

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
```

Number of authentication requests 2228536 - - - - - >>>> Unusual increments

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
```

Number of rejects 2225363 - - - - - >>>> Unusual increments / Unusual rejection rate

```
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

توصيات

فكر في التوصيات التالية وطبقها.

1. تمكين التسجيل.

التسجيل هو جزء مهم من أمن الإنترنت الذي يتضمن تسجيل الأحداث التي تحدث داخل النظام. ويترك عدم وجود سجلات مفصلة ثغرات في الفهم، مما يعوق إجراء تحليل واضح لطريقة الهجوم. يوصى بتمكين التسجيل إلى خادم syslog عن بعد لتحسين إرتباط ومراجعة حوادث الشبكة والأمان عبر أجهزة الشبكة المختلفة.

للحصول على معلومات حول كيفية تكوين التسجيل، راجع الأدلة التالية الخاصة بالنظام الأساسي:

برامج Cisco ASA:

- استخدام الدليل لتأمين جدار حماية ASA
- فصل التسجيل من دليل تكوين واجهة سطر الأوامر الخاصة بالعمليات العامة Cisco Secure Firewall ASA Series General Operations CLI

برنامج FTD من Cisco:

- تكوين تسجيل الدخول إلى FTD من خلال مركز إدارة جدار الحماية (FMC)
- تكوين قسم syslog في فصل إعدادات النظام الأساسي من دليل تكوين جهاز مركز إدارة جدار الحماية الآمن من Cisco
- تكوين syslog والتحقق من صحته في FirePOWER Device Manager
- تكوين قسم إعدادات تسجيل النظام في فصل إعدادات النظام من دليل تكوين الدفاع عن تهديد FirePOWER لـ FirePOWER

ملاحظة: يجب تمكين معرفات رسائل syslog اللازمة للتحقق من السلوكيات الموضحة في هذا المستند (716039 و 113005 و 113015) على مستوى المعلومات (6). وتندرج هذه المعرفات ضمن فئات التسجيل "المصادقة" و"webVPN".

---

2. تكوين ميزات اكتشاف التهديدات أو تدابير التعزيز للوصول عن بعد إلى VPN.

للمساعدة في تخفيف التأثير وتقليل أحتمالية حدوث هجمات القوة الغاشمة هذه على إتصالات الشبكة المحلية الظاهرية (RAPN) لديك، يمكنك مراجعة خيارات التكوين التالية وتطبيقها:

الخيار 1 (المفضل): تكوين اكتشاف التهديدات لخدمات VPN للوصول عن بعد.

تتيح لك ميزات اكتشاف التهديدات للوصول عن بعد إلى خدمات VPN الحماية ضد هذا النوع من الهجمات من خلال حظر المضيف (عنوان IP) الذي يتجاوز الحدود التي تم تكوينها تلقائيا، لمنع مزيد من المحاولات حتى تقوم بإزالة فجوة عنوان IP يدويا.

يتم دعم ميزات اكتشاف التهديدات هذه حاليا في إصدارات جدار الحماية الآمن من Cisco المدرجة في القائمة التالية:

برامج ASA:

- قطار الإصدار 9.16 -> مدعوم من الإصدار 9.16(4)67 والإصدارات الأحدث داخل هذا القطار المحدد.
- قطار الإصدار 9.18 -> مدعوم من الإصدار 9.18(4)40 والإصدارات الأحدث داخل هذا القطار المحدد.
- قطار النسخة 9. 20 -> مدعوم من الإصدار 9. 20 (3) والإصدارات الأحدث داخل هذا القطار المحدد.
- قطار الإصدار 9.22 -> مدعوم من الإصدار 9.22(1.1) وأي إصدارات أحدث.

برنامج FTD:

- قطار الإصدار 7.0 -> مدعوم من الإصدار 7.0.6.3 والإصدارات الأحدث ضمن هذا القطار المحدد.
- قطار الإصدار 7.6 -> مدعوم من الإصدار 7.6.0 وأي إصدارات أحدث.

ملاحظة: هذه الميزات غير مدعومة حاليا في الإصدار trains 7.1 أو 7.2 أو 7.3 أو 7.4. يتم تحديث هذا المستند بمجرد توفرها.

للحصول على التفاصيل الكاملة وإرشادات التكوين، يرجى الرجوع إلى المستندات التالية:

- التكوين على Secure Firewall ASA: تكوين اكتشاف التهديدات للوصول عن بعد VPN على Secure Firewall ASA.
- التكوين على Secure Firewall FTD: تكوين اكتشاف التهديدات للوصول عن بعد إلى خدمات VPN على الدفاع الآمن عن تهديد جدار الحماية

الخيار 2: تطبيق تدابير التعزيز للوصول عن بعد إلى VPN.

إذا لم تكن ميزات اكتشاف التهديدات لخدمات VPN للوصول عن بعد مدعومة في إصدار جدار الحماية الآمن الخاص بك، فقم بتنفيذ جميع تدابير التعزيز التالية لتقليل تأثير هذه الهجمات:

1. تعطيل مصادقة AAA في DefaultWebVPN وتوصيفات توصيل DefaultRagGroup (خطوة بخطوة: ASA | تتم إدارة برنامج الإرسال فائق السرعة (FTD) بواسطة FMC).
2. تعطيل وضع جدار الحماية الآمن (Hostscan) من DefaultWEBvpngGroup و DefaultRAGgroup (خطوة بخطوة: ASA | تتم إدارة برنامج الإرسال فائق السرعة (FTD) بواسطة FMC).
3. تعطيل أسماء المجموعات المستعارة وتمكين عناوين URL الخاصة بالمجموعات في ملفات تعريف الاتصال (خطوة بخطوة: ASA | تتم إدارة برنامج الإرسال فائق السرعة (FTD) بواسطة FMC).

ملاحظة: إذا كنت بحاجة إلى دعم عن طريق برنامج الإرسال فائق السرعة (FTD) الذي تتم إدارته من خلال إدارة أجهزة جدار الحماية المحلية (FDM)، فيرجى الاتصال بمركز المساعدة التقنية (TAC) للحصول على إرشادات الخبراء.

للحصول على مزيد من التفاصيل، يرجى الرجوع إلى دليل تنفيذ تدابير التعزيز لبروتوكول AnyConnect VPN الآمن الخاص بالعميل.

الخيار 3: حظر محاولات الاتصال يدويا من مصدر ضارة.

من أجل منع محاولات الاتصال من مصدر غير مصرح لها، يمكنك تنفيذ أي من الخيارات المدرجة أدناه:

- أستخدم الأمر "shun":

هذا أسلوب واضح لحظر بروتوكول الإنترنت خبيث، ولكن، يجب أن يتم يدويا. الرجاء قراءة المقطع التكوين اليدوي لحظر الهجمات على جدار الحماية الآمن باستخدام الأمر 'shun' للحصول على مزيد من التفاصيل.

- تكوين قائمة التحكم في الوصول إلى مستوى التحكم:

تطبيق قائمة التحكم في الوصول (ACL) على ASA/FTD لتصفية عناوين IP العامة غير المصرح بها ومنعها من بدء جلسات عمل VPN البعيدة. تكوين سياسات التحكم في الوصول إلى مستوى التحكم للدفاع الآمن عن تهديد جدار الحماية و ASA.

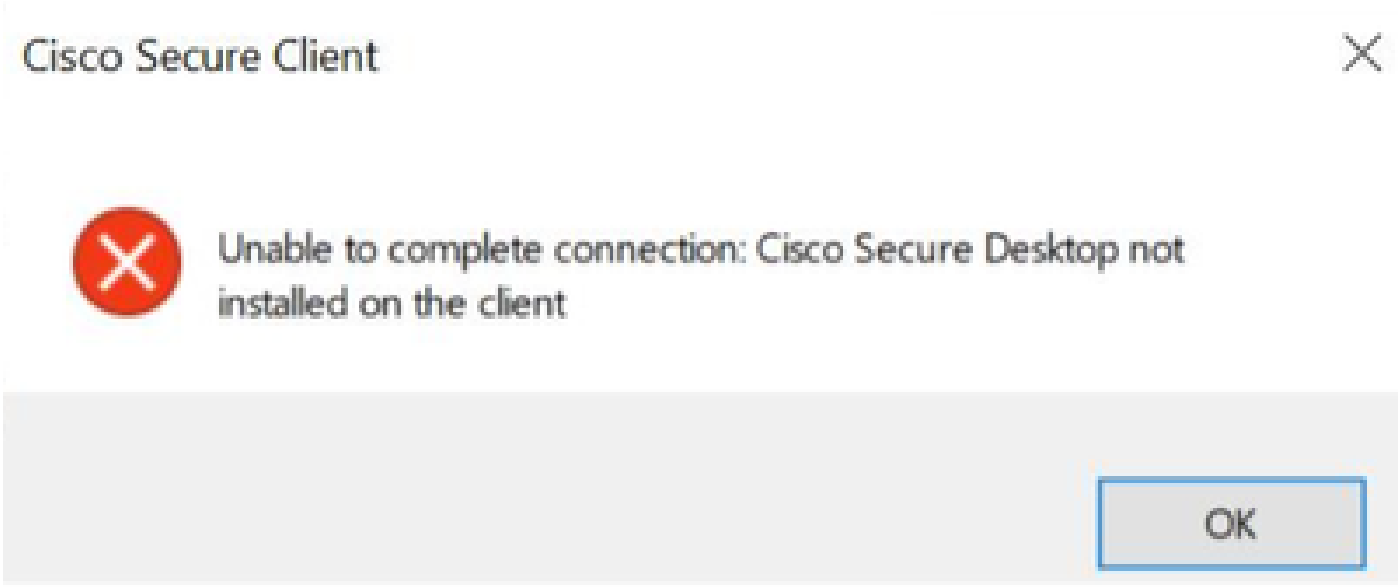
ملاحظة: قام Cisco Talos بنشر قائمة بعناوين IP وبيانات الاعتماد المرتبطة بهذه الهجمات. يمكن العثور على رابط لمستودع GitHub الخاص بهم في قسم "IOCs" من الاستشارات الخاصة بهم. من المهم ملاحظة أن عناوين IP للمصدر لحركة المرور هذه من المرجح أن تتغير، لذلك، يجب عليك مراجعة سجلات الأمان (syslog) لتحديد عناوين IP التي تحتوي على مشاكل. عند تحديد الهوية، يمكن إستخدام أي من الخيارات الثلاثة لحظرها.

السلوكيات ذات الصلة

هناك أعراض معينة يمكن إختبارها تتيجة لاستهداف جدار الحماية الآمن بواسطة هجمات رش كلمة المرور. لحل هذه المشاكل، النظر في تنفيذ التوصيات الواردة في هذه الوثيقة.

العرض الجانبي 1: يتعذر إنشاء إتصالات VPN مع عميل Cisco الآمن (AnyConnect) عند تمكين وضع جدار الحماية (HostScan)

عند محاولة إنشاء اتصال RAPN باستخدام عميل Cisco الآمن (AnyConnect)، يمكن للمستخدمين مواجهة رسالة خطأ بشكل متقطع تذكر، "غير قادر على إكمال الاتصال. لم يتم تثبيت "سطح المكتب الآمن من Cisco" على العميل.". ينشأ هذا السلوك عادة عندما يكون هناك فشل في تخصيص رمز مميز للمسح الضوئي بواسطة وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN)، إما ASA أو FTD لجدار الحماية الآمن من Cisco. ومن الجدير بالذكر أن فشل التخصيص هذا يرتبط بحالات الهجمات العنيفة التي تستهدف البنية الأساسية لجدار الحماية الآمن ويحول دون الإكمال الناجح لعملية اتصال الشبكة الخاصة الظاهرية (VPN). تم تعقب هذا السلوك وحله عبر معرف تصحيح الأخطاء من Cisco CSCwj45822.



ملاحظة: لا يحدث هذا السلوك المحدد إلا عند تمكين وضع جدار الحماية (HostScan) عند إصدار AnyConnect أو Secure Client، بغض النظر عن استخدام وحدة الاستقبال والبث.

لتأكيد ما إذا كانت وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN) تعرض أعراض حالات فشل تخصيص الرمز المميز للتحميل، قم بتشغيل الأمر debug list webVPN 187 0.

```
<#root>

ASA# debug menu webvpn 187 0
```

```
Allocated Hostscan token = 1000
```

Hostscan token allocate failure = xxx - - - - > Increments

ملاحظة: يأتي حدوث هذه المسألة نتيجة للهجمات. تم تعقب هذا السلوك وحله عبر معرف تصحيح الأخطاء من Cisco CSCwj45822.

لحل هذه المشكلة، ضع في الاعتبار تنفيذ التوصيات الواردة في هذا المستند.

تطبيقات التعزيز الإضافية ل RAVPN

يمكنك التفكير في إتخاذ تدابير مضادة إضافية تتطلب تغييرات إضافية على عمليات النشر الخاصة بك لتعزيز أمان نشر الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد، مثل اعتماد مصادقة قائمة على الشهادة ل RAPN. يرجى الرجوع إلى مستند تنفيذ تدابير التعزيز لعميل AnyConnect VPN الآمن للحصول على إرشادات التكوين التفصيلية.

معلومات إضافية

- إجراءات التحقيق الجنائي ل Cisco ASA للمستجيبين الأوائل
- إجراءات التحقيق الجنائي للدفاع عن التهديد الذي تشكله Cisco للمستجيبين الأوائل
- إخطارات تهديد Telos من Cisco
- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات اتصال دعم Cisco في جميع أنحاء العالم.

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).