الحل البديل والكشف من جانب العميل للهجوم على الحامل اللاسلكي

المحتويات

المقدمة

في 16 أكتوبر/تشرين الأول، تم الإعلان عن مجموعة من نقاط الضعف المعروفة على نطاق واسع باسم KRACK والتي تؤثر على البروتوكولات المختلفة المستخدمة في شبكات WPA/WPA2، والتي يمكن أن تضر بخصوصية البيانات أو تكاملها عند إرسالها عبر اتصال لاسلكي. وهي تؤثر على بروتوكولات الأمان المستخدمة على شبكات WiFi.

ويختلف المستوى العملي للتأثير إختلافا كبيرا على كل سيناريو، بالإضافة إلى عدم تأثر جميع عمليات التنفيذ من جانب العملاء بنفس الطريقة.
تستخدم الهجمات سيناريوهات ذكية مختلفة من "الاختبار السلبي" حيث تتم تجربة عمليات انتقال الحالة التي لم يتم تعريفها بشكل صحيح على المعايير اللاسلكية، وفي معظم الحالات ال يتم التعامل معها بشكل صحيح بواسطة الجهاز المتأثر. وهو ال يتعارض مع خوارزميات التشفير المستخدمة لحماية WPA2، بل حول كيفية إجراء مفاوضات المصادقة والبروتوكول أثناء تأمين التوصيل اللاسلكي.

تم الإبلاغ عن معظم سيناريوهات الثغرات الأمنية للعملاء، حيث سيستخدم الهجوم النموذجي المحتمل نقاط وصول وهمية ك "رجل في الوسط" لاعتراض وإحداث إطارات محددة أثناء المفاوضات الأمنية بين العميل ونقطة الوصول الحقيقية (CVE-2017-13077، CVE-2017-13078، CVE-2017-13079، CVE-2017-13080، CVE-2017-1300817-1300). هذه هي بؤرة هذا المستند

تم وصف أحد السيناريوهات عند الهجوم على البنية الأساسية لنقطة الوصول التي توفر خدمات التجوال السريع 802. 11r (FT) (CVE-2017-1382)، والتي تم تثبيتها على رمز AireOS الذي تم إصداره مؤخرا

هناك 4 هجمات متبقية ضد بروتوكولات خاصة بالعملاء: STK و TDLS و WNM، التي لا تدعمها مباشرة البنية الأساسية لنظام التشغيل AireOS (CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088)، وهي خارج نطاق هذا المستند

ومن الناحية العملية، يمكن للمهاجم فك تشفير حركة مرور البيانات للجلسة المتأثرة، أو حقن إطارات في إتجاه واحد أو إتنين . كما أنها لا توفر طريقة لفك تشفير حركة المرور الموجودة سابقا، قبل الهجوم، كما أنها لن توفر آلية "للحصول" على كالمات تشفير لجميع الأجهزة في SSID معينة أو كلمات المرور PSK أو 802.1x الخاصة بها

إن نقاط الضعف حقيقية ولها تأثير كبير ولكنها لا تعني أن الشبكات المحمية WPA2 "تتأثر إلى الأبد" حيث يمكن إصلاح المشكلة من خلال تحسين عمليات التنفيذ على كل من العميل ونقطة الوصول للعمل بشكل صحيح في *سيناريوهات الاختبار السلبية* التي لا يتم التعامل معها حاليا بطريقة قوية

ما الذي يجب على العميل القيام به:

- بالنسبة لنقاط الضعف الجانبية لنقطة الوصول: تعد الترقية الإجراء المطلوب عند إستخدام FT. إذا لم تكن هناك حاجة إلى FT لخدمات الصوت/الفيديو، فقم بتقييم ما إذا كان يجب تعطيل ميزة FT حتى يتم إجراء الترقية إلى التعليمات البرمجية الثابتة. إذا كنت تستخدم الصوت، قم بتقييم ما إذا كان CCKM ممكنا (يحتاج جانب العميل إلى الدعم)، أو الترقية إلى كود ثابت. في حالة عدم إستخدام FT/802.11r، فلا حاجة للترقية في هذا الوقت
- بالنسبة لنقاط الضعف من جانب العميل، اعمل على تحسين مستوى رؤيتك: تأكد من تمكين الكشف المخادع، الذي يغطي جميع القنوات، ثم قم بإنشاء قاعدة للإبلاغ عن "SSID المدار" كضار. بالإضافة إلى ذلك، قم بتطبيق تغييرات تكوينات إعادة محاولة EAPoL التي يمكنها الحد من الهجمات التي سيتم تنفيذها أو حظرها بالكامل، كما هو موضح في هذا المستند

() المشورة المرجعية الرئيسية هي في
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa. ت

المكونات المستخدمة

يركز هذا المستند على وحدات التحكم اللاسلكية التي تشغل الإصدار 8.0 أو الأحدث.

المتطلبات

والمطلوب معرفة المحتوى الذي تغطيه المشورة الأمنية المذكورة أعلاه.

فيما يتعلق بهجمات WPA KRACK، هناك إجرائان رئيسيان يمكن أن نتخذهما لحماية العملاء الذين لم يتم ترقيتهم بعد.

1. حماية إعادة محاولة EAPoL (EAP عبر LAN)

2. الكشف عن المخادع وميزات انتحال نقاط الوصول (AP)، لاكتشاف ما إذا كانت أدوات الهجوم قيد الاستخدام

أوجه الحماية من هجوم EAPoL

فيما يتعلق بأوجه الضعف-2017-13077 إلى 81، يكون من السهل نسبيا منع تأثر العملاء، باستخدام عداد إعادة محاولة EAPoL المعين على صفر. هذا تشكيل يتوفر في كل WLC صيغة

لماذا ينجح هذا

يحتاج الموجه على الأقل إلى إعادة محاولة EAPoL إضافية واحدة على الأقل أثناء المصافحة رباعية الطرق، أو أثناء تناوب مفتاح البث. إذا قمنا بحظر إنشاء عمليات إعادة المحاولة، لا يمكن تطبيق الموجه على المفتاح المؤقت Pairwise (PTK)/GroupWise Transient Key (GTK).

تأثير محتمل

1. العملاء البطيئون أو الذين قد يسقطون المعالجة الأولية ل EAPoL M1 (أي الرسالة الأولى لتبادل مفتاح الطريق الرابع). وهذا يظهر على بعض العملاء الصغار أو بعض الهواتف، والتي قد تتلقى M1، ولا تكون جاهزة لمعالجتها بعد مرحلة مصادقة dot1x، أو قم بذلك بسبب عطاء شديد لتلبية مؤقت إعادة الإرسال القصير

2. السيناريوهات التي تحتوي على بيئة تردد لاسلكي سيئ، أو إتصالات WAN بين AP و WLC، والتي قد تتسبب في إسقاط الحزمة في نقطة ما على الإرسال نحو العميل.

وفي تلك السيناريوهين، تكون النتيجة أنه قد يتم الإبلاغ عن فشل في تبادل EAPoL، وسيتم إلغاء مصادقة العميل، وسيتعين عليه إعادة تشغيل عمليتي الاقتران والمصادقة.

لتقليل إحتمالية ظهور المشكلة في هذه المشكلة، يجب إستخدام مهلة أطول (1000 مللي ثانية)، للسماح بمزيد من الوقت للعملاء البطيئين في الاستجابة. الإعداد الافتراضي هو 1000 مللي ثانية، ولكن يمكن تغييره إلى قيمة أقل يدويا بحيث يتم التحقق منه.

التكوين

هناك آليتان متاحتان لتكوين هذا التغيير.

- عمومي، متوفر في جميع الإصدارات
- لكل شبكة محلية لاسلكية (WLAN)، متوفرة من 7.6 إلى الأحدث

الشامل خيار بسيط، ويمكن أن يتم في كل إطلاق، التأثير يكون عبر كل WLANs في ال WLC.

يسمح إعداد التكوين لكل شبكة محلية لاسلكية (WLAN) بالتحكم بشكل أكبر متعدد المستويات مع إمكانية الحد من تأثير SSID، بحيث يمكن تطبيق التغييرات لكل أنواع الأجهزة، وما إلى ذلك، إذا تم تجميعها على شبكات محلية لاسلكية (WLAN) معينة. وهذا متاح من الإصدار 7.6

على سبيل المثال، يمكن تطبيقه على شبكة محلية لاسلكية 802.1x عامة، لكن ليس على شبكة محلية لاسلكية (WLAN) خاصة بالصوت، حيث قد يكون لها تأثير أكبر

التكوين العام الأول:

```
config advanced eap eapol-key-retries 0
```

(خيار CLI فقط)

يمكن التحقق من صحة القيمة من خلال:

```
(2500-1-ipv6) >show advanced eap

EAP-Identity-Request Timeout (seconds)..... 30

EAP-Identity-Request Max Retries.............. 2

EAP Key-Index for Dynamic WEP................. 0

EAP Max-Login Ignore Identity Response..... enable

EAP-Request Timeout (seconds)................. 30

EAP-Request Max Retries....................... 2

EAPOL-Key Timeout (milliseconds)............... 1000

EAPOL-Key Max Retries......................... 0

EAP-Broadcast Key Interval.................... 3600
```

الشركة الثانية في تكوين الشبكة المحلية اللاسلكية (WLAN)

X=معرف WLAN

```
config wlan security eap-params enable X

config wlan security eap-params eapol-key-retries 0 X
```

كيفية تحديد ما إذا تم حذف عميل بسبب عدم إعادة الإرسال على الإطلاق

سوف يتم حذف العميل بسبب الحد الأقصى من عمليات إعادة محاولة EAPoL التي تم الوصول إليها، والتي تم إلغاء المصادقة عليها. عدد مرات إعادة الإرسال هو 1، حيث يتم حساب الإطار الأولي

```
 *Dot1x_NW_MsgTask_6: Oct 19 12:44:13.524: 28:34:a2:82:41:f6 Sending EAPOL-Key Message to mobile
28:34:a2:82:41:f6
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
..
*osapiBsnTimer: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 802.1x 'timeoutEvt' Timer expired for
station 28:34:a2:82:41:f6 and for message = M3
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.042: 28:34:a2:82:41:f6 Retransmit failure for EAPOL-Key M3
to mobile 28:34:a2:82:41:f6, retransmit count 1, mscb deauth count 0
..
*Dot1x_NW_MsgTask_6: Oct 19 12:44:14.043: 28:34:a2:82:41:f6 Sent Deauthenticate to mobile on
BSSID 58:ac:78:89:b4:19 slot 1(caller 1x_ptsm.c:602)
```

اكتشاف المخادع

يحتاج العديد من تقنيات الهجوم لنقاط الضعف أمام تشفير PMK/GTK العميل إلى "تقديم" نقطة وصول مزورة بنفس SSID لنقطة الوصول للبنية الأساسية، لكنها تعمل في قناة مختلفة. يمكن اكتشاف ذلك بسهولة ويمكن لمسؤول الشبكة إتخاذ إجراءات فعلية تستند إليه، نظرا لأنه نشاط مرئي.

هناك طريقتان مقترحتان حتى الآن لتنفيذ هجمات EAPoL :

- تزييف البنية التحتية AP، بمعنى آخر، العميل نقطة وصول مخادعة، باستخدام نفس عنوان MAC، لنقطة وصول حقيقية، لكن على قناة مختلفة. سهل التنفيذ للمهاجم لكنه ظاهر للعيان
- حقن الإطارات في اتصال صحيح، مما يجبر العميل على الاستجابة. وهذا أقل وضوحا بكثير، ولكن يمكن اكتشافه في بعض الظروف، وقد يحتاج إلى توقيت دقيق جدا ليكون ناجحا

ويمكن أن يؤدي الجمع بين ميزات انتحال نقاط الوصول والكشف عن المخادع إلى كشف ما إذا كان يتم وضع "نقطة وصول مزيفة" في الشبكة.

التكوين

- تحقق من تمكين الكشف المخادع على نقاط الوصول. يتم تمكين هذا بشكل افتراضي، ولكن قد يكون تم تعطيله يدويا بواسطة المسؤول، لذلك يجب التحقق منه.

- قم بإنشاء قاعدة وضع عالمة على المخادعين باستخدام "SSIDs المدارة" كمخاطرة:

- تأكد من تعيين مراقبة القناة على "جميع القنوات" لكل من شبكات 802.11a/b. تم تصميم الهجوم الأساسي ليكون قريبا من منظور التردد اللاسلكي (RF)، العميل، على قناة مختلفة عما يتم إستخدامه على نقاط الوصول (APs) للبنية الأساسية. لهذا السبب من المهم التأكد من مسح كل القنوات الممكنة ضوئيا:

انتحال نقطة الوصول

عند التهيئة الافتراضية، يمكن للبنية الأساسية اكتشاف ما إذا كانت أداة الهجوم تستخدم أحد عناوين MAC الخاصة بنقطة الوصول. يتم الإبلاغ عن ذلك على أنه فخ SNMP وسيكون مؤشرا على أن الهجوم يحدث.

```
Impersonation of AP with Base Radio MAC bc:16:65:13:a0:40 using source address of
bc:16:65:13:a0:40 has been detected by the AP with MAC Address: bc:16:65:13:a0:40 on its
802.11b/g radio whose slot ID is 0
```

المراجع

إشعار استشاري أمني

المادة المخادعة في شبكة اللاسلكية الموحدة باستخدام الإصدار 7.4 - Cisco

أفضل ممارسات تكوين وحدة تحكم الشبكة المحلية اللاسلكية من Cisco - Cisco

الكشف المخادع بموجب الشبكات اللاسلكية الموحدة - Cisco

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).