أستكشاف أخطاء عمليات عزل PVO المركزية وإصلاحها على ESA و SMA

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف مشكلات التوصيل والاتصال وإصلاحها عند تمكين السياسات المركزية والفيروسات والحالات التي ينتشر فيها الوباء.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز ESA (Email Security Appliance) مع AsyncOS 8.1 أو إصدار أحدث
- جهاز إدارة الأمان (SMA) باستخدام AsyncOS 8.0 أو إصدار أحدث

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

تم إدخال ميزة الحجر الصحي للسياسة المركزية والفيروسات والتفشي (PVO) في 8.1 / AsyncOS 8.0 (ESA) SMA)). تتضمن هذه الميزة متطلبات اتصال شبكة إضافية، وتطرح بعض التحديات الجديدة لاستكشاف الأخطاء وإصلاحها.

فهم التواصل

- يستخدم اتصال CPQ بروتوكول SMTP، لكن مع بعض الأوامر الإضافية لنقل البيانات الأولية
- سوف تنصت SMA إلى الاتصالات على الواجهة والمنافذ المحددة في الخدمات المركزية -> السياسة والحجر الصحي للفيروسات والتفشي. بشكل افتراضي، الميناء هو 7025، غير أن هذا ربما يكون قد تم تغييره من قبل المستخدم المسؤول!

- وستصغي وكالة الفضاء الأوروبية إلى الاتصالات على الواجهة والميناء المحددين في إطار الخدمات الأمنية -> السياسة، والفيروسات، والحجر الصحي من الفاشية. مرة أخرى، افتراضيا، الميناء هو 7025، غير أن هذا أمكن كنت غيرت ب الإدارة مستعمل!
- كما تستخدم SMA SSH (عبر عميل الأوامر) للحصول على معلومات التكوين من ESAs. وبشكل خاص، يستخدم هذا عندما تقوم SMA بتسليم رسائل البريد الإلكتروني الصادرة إلى ESA. ستستخدم SMA SSH للاستعلام عن تكوين ESA وتحديد الواجهة / المنفذ الذي سيتم تسليم البريد الإلكتروني الذي تم إصداره إليه.

مستمعين

- سيكون لكل من ESA و SMA مستمع مخفي يسمى "cpq_listener" والذي سينصت على المنفذ المحدد. ويمكن ملاحظة هذه المستمعين في ملف التكوين. على سبيل المثال:

```
                                                <listener>
                                    <listener_name>cpq_listener</listener_name>
                                                <protocol>CPQ</protocol>
                                <interface_name>Incoming Mail</interface_name>
                                                    <port>7025</port>
                                        <listen_queue_size>50</listen_queue_size>
                                                <type>private</type>
                                                    <hat>
                                                      RELAYED$
                                                    {} RELAY
                                                      BLOCKED$
                                                  {} REJECT
                                                    :RELAYLIST
                                                    10.1.2.3
                            (RELAYED (Only select hosts can relay from this box$
                                                            ALL
                                                (BLOCKED (Everyone else$
                                                        <hat/>
                                                        <rat>
                                                    <rat_entry>
                                            <rat_address>ALL</rat_address>
                                                <access>ACCEPT</access>
                                                    <rat_entry/>
                                                        <rat/>
```

- سيتم إيقاف هذه المستمعين مؤقتا إذا أستخدم المستخدم المسؤول 'Suspendlisteners all' أو 'Suspend'. إذا كان المنفذ لا يقبل الاتصالات، فيجب التحقق مما إذا كانت حالة النظام 'غير متصلة' والاستئناف إذا لزم الأمر.

أستكشاف أخطاء التسليم وإصلاحها من ESA إلى SMA

- تحقق من إمكانية اتصال ESA ب SMA على المنفذ والواجهة اللذين تم تكوينهما. ويمكن القيام بذلك باستخدام برنامج Telnet. يجب أن تحصل على شعار 220 إذا كان الاتصال ناجحا.
- سيكون لدى ESA كائن وجهة يسمى 'the.cpq.host'، يحتوي على رسائل أثناء وضعها في قائمة الانتظار للتسليم إلى SMA. يمكنك رؤية هذا باستخدام 'tophosts' أو Monitor -> حالة التسليم. لا يمكنك إستخدام 'hoststatus' معه، ولكن يمكنك إستخدام 'showRecipients' و'deleterecipients' إذا لزم الأمر.

أستكشاف أخطاء التسليم وإصلاحها من SMA إلى ESA

- تحقق من إمكانية اتصال SMA ب ESA على المنفذ والواجهة اللذين تم تكوينهما. مرة أخرى، يمكنك إستخدام برنامج Telnet وسوف ترى شعار 220 إذا كان ناجحا.
- وعند إستخدام المجموعات، من المهم أن تكون الواجهة المحددة على مستوى المجموعات في إطار الخدمات الأمنية -> الحجر الصحي الخاص بالسياسات والفيروسات والتفشي موجودة لجميع الأجهزة على مستوى

الأجهزة. (تحقق من الشبكة -> واجهات IP).
- سيكون ل SMA كائن وجهة يسمى 'the.cpq.release.host' يحتوي على رسائل تم إصدارها أثناء وضعها في قائمة الانتظار للتسليم إلى ESA. يمكنك رؤية هذا باستخدام 'tophosts'. لا يبدو أن هذا يعمل مع 'hoststatus' أو 'showrecipients'، ولم أقم باختبار 'deleterecipients' به، ولكن هذا على الأرجح لا يعمل أيضا.
- قد تكون هناك أيضا مشكلات تتعلق باتصال SSH بين SMA و ESA. لا تكون هذه المشكلات دائما مبنية على الشبكة بالضرورة، على سبيل المثال في CSCus29647 ينقطع المكون الداخلي ل SMA عن العمل. عادة ما تظهر مثل هذه المشكلات كأخطاء تطبيقات في سجلات البريد، ويمكن حلها عادة من خلال إعادة تشغيل SMA.

TLS/الشهادات

- تعتمد جميع إتصالات CPQ في أي من الاتجاهين على TLS، ونتيجة لذلك يمكن أن يلعب تكوين تشفير دورا.
- من أجل نجاح اتصال TLS، يجب أن يكون الجهاز الذي يفتح الاتصال قادرا على التحقق من أن الجهاز المتلقي يستخدم شهادة CPQ الخاصة بنا. من الممكن أن يفشل ذلك إذا تفاوض الجهاز على تشفير مجهول. هذا قد يظهر في السجلات على أنه شيء مثل هذا:

```
Mon Apr  1 12:00:00 2014 Info: New SMTP DCID 123456 interface 10.0.0.2 address 10.0.0.1 port
7025
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS failed: verify error: no certificate from
server
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS was required but could not be successfully
negotiated
```

- يمكنك إصلاح هذه المشاكل عن طريق إزالة شفرة مجهول من قائمة شفرة التسليم الصادرة ببساطة، والتي يتم تنفيذها بإضافة '-aNULL:' إلى نهاية قائمة الشفرة. على سبيل المثال: high:medium:**-aNULL**

ملف السجل

- إذا كان لدى SMA اشتراك في سجلات البريد (يتم ذلك بشكل افتراضي)، يمكنك مراجعة سجلات البريد لتجميع معلومات إضافية.
- ستبدو أحداث تلقي CPQ بهذا الشكل بالنسبة إلى كل من الرسائل التي يتم وضعها في الحجر الصحي على "الإدارة العسكرية الأمريكية" والرسائل التي يتم إصدارها إلى ESA

```
New CPQ ICID 12345 interface Management (10.10.10.1) address 10.10.20.1 reverse dns host
unknown verified no
```

- يمكنك البحث عن هذه الأحداث باستخدام GREP، مثال: GREP "CPQ ICID" mail_log
- تبدو أحداث توصيل المعالج CPQ، سواء من خلال الحجر الصحي من ESA أو من خلال الإصدار من الفحص الصحي من SMA، مماثلة لأي عملية تسليم أخرى، باستثناء أنه يتم إدراج المنفذ المخصص وبعض الأسطر تتضمن الكلمة "عزل السياسة المركزية". المثال التالي:

```
Fri Sep 13 15:08:02 2013 Info: New SMTP DCID 12345 interface 10.10.20.1 address 10.10.10.1
port 7025
Fri Sep 13 15:08:02 2013 Info: DCID 12345 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Fri Sep 13 15:08:02 2013 Info: Delivery start DCID 12345 MID 23456 to RID [0] to Centralized
Policy Quarantine
Fri Sep 13 15:08:02 2013 Info: Message done DCID 12345 MID 23456 to RID [0] (centralized
(policy quarantine
Fri Sep 13 15:08:07 2013 Info: DCID 12345 close
```

• أنت يستطيع وجدت هذا حادث باستخدام GREP أن يحدد للميناء، مثال: GREP "ميناء 7025" mail_log
زر 'enable' ESA معطل

عند محاولة تمكين PVO على ESA، قد تجد أن زر "تمكين" قد تم سحبه بالكامل، على الرغم من إكمال كافة عمليات التكوين المطلوبة مسبقا. عندما يعرض ESA صفحة PVO، فإنه يتصل ب SMA عبر المنفذ 7025 للتحقق من أن التكوين جاهز ليتم تمكينه. في حالة فشل هذا الاتصال، سيتم تعطيل الزر 'enable'. أنت يستطيع تحريت هذا تماما مثل أي SMA -> ESA ميناء 7025 إتصال ب يثبت ل "ميناء 7025" على ال ESA. للحصول على مزيد من المعلومات، ارجع إلى الملاحظة الفنية المدرجة في المعلومات ذات الصلة.

معلومات ذات صلة

- متطلبات معالج ترحيل PVO عندما تكون ESA مجمعة
- لا يمكن تمكين عزل السياسة والفيروسات والفاشيات (PVO) مركزيا ل ESA

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).