تأثير فحص الطبقة 7 على حركة المرور متعددة الطبقات: إستعراض تنفيذ برنامج SNORT3

المحتويات

مسألة

بعد تمكين قواعد DNS Sinkhole في سياسة التحكم في الوصول (ACP)، بدأت حركة مرور FirePOWER المدية عن تهديد أجهزة الدفاع على توقع غير بشكل السقوط في المغلفة VXLAN snort 3. محرك إصدارات إلى تشغل التي (FTD)

· قامت شبكة VXLAN بتضمين عمليات إسقاط حركة مرور البيانات بعد تمكين سياسة فتحة أمان DNS.

· أحداث الاتصال التي تظهر عناوين IP الداخلية (على سبيل المثال، 100.70.x.x) بدلا من .الخارجية VXLAN رؤوس

· تم العثور على سلوك غير متوقع أثناء تنفيذ Snort 3 أثناء الاختبار المعملي.

البيئة

•النظام الأساسي: زوج FTD عالي التوفر (HA)

· الإصدار المتأثر: 7.6.2.1 (Snort 3)

· الإصدار الثابت: 7. 6. 4+ (شورت 3)

قارن

الحل في 7.6.2.1:

##########

الخطوة 1:

(مستحسن) قم بإنشاء قاعدة PreFilter لتجاوز فحص الشعاع لحركة مرور VXLAN:

· نهج التصفية المسبقة

•الإجراء: مسار سريع (قاعدة النفق)

· المصدر: <External_VXLAN_SOURCE_IPs>

•الوجهة: <External_VXLAN_DESTINATION_IPs>

•البروتوكول: UDP

•المنفذ: 4789

الخطوة 2:

مسح الاتصالات الموجودة

· مسح عنوان المحتوى <external_ip_1> وعنوان <external_ip_2>

قم بضبط ترتيب القواعد في حالة عدم إستخدام نهج عامل التصفية المسبق

.ACP في IP لـ الداخلية السماح قواعد قبل (DNS Sinkhole، App-ID) L7 قواعد ضع

الحل طويل الأجل:

##########

1. الترقية إلى FTD 7.6.4 أو إصدار أحدث

· حل CSCwo54753 (خلل PSIR)

· توفير سلوك فحص متناسق متعدد الطبقات.

2. قم بتكوين كل من القواعد الداخلية والخارجية لثقب DNS:

· عند إستخدام DNS Sinkhole أو ميزات أخرى لذكاء الأمان مع حركة مرور مغلفة.

3. بالنسبة للميزات من المستوى السابع بخلاف SI (تصفية عنوان URL والتحكم في التطبيق):

· قواعد الرأس الداخلي فقط مطلوبة في ACP.

· قواعد الرأس الخارجي غير ضرورية.

مزيد من التفاصيل حول ميزة فحص شبكة VXLAN متعددة الطبقات

##

يتضمن برنامج الإرسال فائق السرعة (FTD) إمكانية فحص متعددة الطبقات للحصول على سرعة 7. تحدد هذه الميزة ما إذا كان Snort يفحص رؤوس ومعلومات الأمان (SI) من الطبقة 7 التي تم تكوينها. التضمين الخارجي أو رؤوس الحمولة الداخلية استنادا إلى نهج الطبقة 7.

تتضمن ميزات المستوى 7 ما يلي:

· فتحة أمان DNS

· التحكم في التطبيق (App-ID)

· تصفية URL

· الموقع الجغرافي

· منع التسلل

سلوك المفتاح:

########

ينتقل ،(ACP) لوصول في قائمة التحكم في الطبقة 7 من ميزة تمكين أي تم عندما
الشرخ إلى فحص الرؤوس الداخلية للحزم المغلفة (على سبيل المثال، VXLAN، GRE، IP-in-
IP).

التحليل الفني:
##########
Snort 3 (7.6.2.1) - سلوك معيب

بدون قواعد الطبقة 7:

· يعتمد snort على بيانات تعريف الاتصال من Lina (محرك بيانات ASA).

· يتم السماح بحركة المرور/رفضها استنادا إلى قواعد الرأس الخارجي فقط.

· لم يتم إجراء فحص الرأس الداخلي.

مع قواعد الطبقة 7:

· إجراء عمليات فحص ACP وفرض الفحص متعدد الطبقات.

· الأمور المتعلقة بأمر القاعدة (العيب في الشروت 3).

· إذا ظهرت قاعدة IP الداخلية قبل إسقاط حركة مرور → VXLAN لقاعدة L7 —> السلوك المعيب

مخرجات المختبر:
طاقم — L7 قاعدة بقاعدة متبوعة IP ل الداخلية ACP قاعدة — snort3 — 7.6.2.1 — LAB FTD

تفاصيل متعقب حزم البيانات المعملية:

17:46:48.773778 10.142.133.15:36066>10.126.133.15:4789 udp 80

Inside(vrfid:0)

Object_group_search

وضع NGIPS

NGIPS عضو |

قائمة الوصول

ngips-egress-interface-lookup

| حل واجهة الخروج

إنشاء التدفق

فحص خارجي

SNORT

النوع:

SNORT

النتيجة:

قطرة

التكوين:

الوقت المنقضي:

81472 نانو ثانية

معلومات إضافية

النتيجة: قطرة

واجهة الإدخال:

Inside(vrfid:0)

حالة الإدخال:

لمعي

:حالة سطر الإدخال

لمعي

:واجهة الإخراج

خارج(vrfid:0)

:حالة الإخراج

لمعي

:حالة سطر الإخراج

لمعي

:الإجراء

قطرة

:الوقت المستغرق

928908 نانو ثانية

:سبب الإسقاط

سبب الإسقاط <— تم حظره بواسطة معالج مسبق لجدار الحماية (جدار الحماية)

:تفاصيل الإسقاط

موقع الإفلات: فحص الإطارات_dp_snort_snp_drop_frame_wcaller:58 flow (NA)/NA

خارج(vrfid:0)

· إذا ظهرت قاعدة L7 قبل ← حركة مرور VXLAN لقاعدة IP الداخلية المسموح بها

سلوك محدد ل DNS Sinkhole (Snort 3):

· تقوم فتحة DNS بتشغيل الفحص متعدد الطبقات حتى عندما يسمح ترتيب القواعد بحركة المرور بطريقة أخرى.

Snort 3 (7.6.4+) - سلوك ثابت

ما بعد الإصلاح (CSCwo54753):

· يتم تمكين الفحص متعدد الطبقات بشكل متناسق عند وجود ميزات L7.

· لا يؤثر ترتيب القاعدة على السلوك.

· يستند فحص حركة المرور إلى رؤوس الأعمدة بغض النظر عن موضع القاعدة.

· يجب السماح بكل من الرأسين الداخلي والخارجي في ACP لسيناريوهات DNS Sinkhole.

مصفوفة مقارنة حالات الاختبار

سيناريو الاختبار	FTD 7.6.2.1 (Snort 3)	برنامج FTD 7. 6. 4+ (إصدار 3)	السلوك المتوقع
قاعدة IP متبوعة بقاعدة L7 الداخلية	مسموح به	مسموح به	حركة المرور المسموح بها
قاعدة IP الداخلية متبعة لقاعدة L7	تم الإسقاط (الخلل)	مسموح به	حركة المرور المسموح بها
قاعدة IP الداخلية فقط (L7 موجود)	محصور	محصور	محظور (لا يوجد تصريح داخلي)
قاعدة IP الخارجية فقط (L7 موجود)	مسموح به	محصور	فحص Snort 3 الرأسي الداخلي
فتحة إضافة IP الخارجية + DNS فقط	محصور	محصور	تفرض قاعدة L7 الفحص الداخلي

فتحة الإضافة الداخلية ل IP + DNS فقط	محصور	محصور	تفرض قاعدة L7 الفحص الداخلي

السبب

يرجع السبب في هذا السلوك إلى إمكانية الفحص متعدد الطبقات التي يتسم بها برنامج Snort 3 لمميزات الذكاء الأمني. عندما يتم تمكين فتحة DNS (جزء من ذكاء الأمان)، يقوم Snort 3 بفحص حزمة عميق يقوم باكتشاف عناوين IP الداخلية وتقييمها داخل الحزم التي تم تغليفها، بغض النظر عن طبقة النقل.

وثيقت الإصدار في cisco بق id CSCwt12564، أي يذكر: "إذا كنت تستخدم شرط L7 (تصفية معلومات في القاعدة أو ميزة إلى ذلك) في القاعدة، وتحديد الموقع الجغرافي وما إلى ذلك، ومعرف التطبيق، و url، فأنت بحاجة إلى قاعدة ACP مع رأس داخلي في قائمة التحكم بالوصول (ACP)، لكل SI، يلزم توفر DNS في سياسة DNS، التي تعد جزءا من ذكاء الأمان. مع وجود فتحة DNS، حتى تتطابق القواعد. يتطابق (ACP) في الوصول في قائمة التحكم في الخارجي والداخلي الرأس من

يختلف هذا السلوك عن العملية العادية حيث يتم تقييم الرؤوس الخارجية فقط لحركة مرور VXLAN العابرة عند عدم تكوين ميزات الطبقة 7 أو ذكاء الأمان.

المحتوى ذي الصلة

- دليل تكوين Snort 3
- الدعم الفني والتنزيلات من Cisco
- معرف تصحيح الأخطاء من Cisco CSCwt12564
- معرف تصحيح الأخطاء من Cisco CSCwt07320
- معرف تصحيح الأخطاء من Cisco CSCwu75396
- معرف تصحيح الأخطاء من Cisco CSCwt58320

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).