أستكشاف أخطاء حظر عناوين IP الخاصة من قبل FTD وإصلاحها بسبب مشكلة في التحليل SI

المحتويات

مسألة

بدأت أجهزة FTD في حظر حركة مرور الإنتاج الداخلية عندما يحتوي مضيف URL على عنوان IP خاص بعد تلقي تحديثات موجز ويب URL/الشبكة ذكاء الأمان من Talos.

تتضمن حركة المرور المتأثرة عناوين URL مثل http://10.54.1.7:8200/v1/sys/health وhttp://172.31.14.7:9100. يتم تصنيف حركة المرور إلى "عناوين IP الخاصة كمضيف"، كما تم حظرها بواسطة سياسات المعلومات الأمنية ذات الصلة بنظام التشغيل Talos مع إصدار أحكام تشمل "URL Block" و"BlackList" و"si، force_block". يؤثر هذا السلوك على إتصالات الخدمة الداخلية وعمليات العمل.

أثناء فحص آثار دعم نظام الإرسال فائق السرعة (FTD)، تمت ملاحظة سلوك الحظر هذا:

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Firewall: allow rule, 'Access_Rule', allow
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Generating an EOF event with rule_id = 26845
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 SI: URL security intelligence list id 104862
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict: blacklist
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict Reason: si, force_block
```

البيئة

- Cisco FTD، الإصدار 7.6.4 (تتم إدارة FMC)
- تم تمكين موجز معلومات ذكاء الأمان مع فئات URL الضارة
- خدمات الإنتاج الداخلية باستخدام عناوين IP الخاصة في عناوين URLs

- حدثت مشكلة بعد تحديثات عنوان URL/موجز ويب ويب لمعلومات الأمان من Talos

فهم سجلات تتبع دعم النظام :

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
```

- في سجلات تتبع دعم النظام، تتم طباعة قيمة الفئة.
- قيمة الفئة : [1048627]
- يتوفر تعيين قيمة الفئة وملف موجز SI المطابق في FTD في الموقع:

الموقع في FTD: /ngfw/var/sf/siurl_download/url.rules

الموقع في ملف Tshoot: /file-contents/var/sf/siurl_download/url.rules

<#root>

kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$

cat url.rules

```
                                # security intelligence manifest file
                   si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048589,white,any
                si,ac0ef862-1cff-11ef-a575-4cf8bc134a1f.lf,1074790408,block,any
                   si,005056bf-1643-0ed3-0000-030068648887.lf,1048646,block,any
                   si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048590,block,any
                   si,c87fe5d4-5868-11ef-8843-a8b3afb1bf74.lf,1048645,block,any
                   si,7c51a74a-d984-11ef-8637-e77eccc0d672.lf,1048649,block,any
                   si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048616,block,any
                   si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048619,block,any
                   si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048620,block,any
                   si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048623,block,any
                   si,8af156ca-8020-4608-9278-01b8745811b7.lf,1048626,block,any
                   si,d3899830-d481-4773-b4e2-7daa7acf8f75.lf,1048633,block,any
                   si,03709ed4-faab-47af-bade-4435f8da11f5.lf,1048615,block,any
                   si,bde824fd-36dd-4a7c-9cc1-80e40ac7db66.lf,1048632,block,any
                   si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048629,block,any
                   si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048625,block,any
                   si,02213098-6d94-4680-8ce8-2d081638d087.lf,1048613,block,any
                   si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048622,block,any
                   si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048621,block,any
                   si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048618,block,any
                   si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048624,block,any
                   si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048617,block,any
                   si,937cf5e8-76d1-4ba2-a83c-475dc80c6976.lf,1048628,block,any
```

```
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048614,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048634,block,any
si,abdc925f-4f85-4504-90a7-c891979af648.lf,1048630,block,any

si,8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf,1048627,block,any >>>>>>matching category ID


si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048631,block,any
si,ac0f6900-1cff-11ef-a575-4cf8bc134a1f.lf,1074790407,monitor,any
ac,5846a44a-3d2a-11f0-a12d-7a89a4a10ab3.lf,1048650
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$ pwd
```

كيفية تفسير السطر (الأسطر) السابق:

- تم تعيين معرف الفئة للمحتوى الموجود في الملف بالاسم "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf": 1048627
- للتحقق من الفئة الفعلية، افتح الملف باستخدام VI أو أي أداة محرر، واسم الفئة يكون في الأعلى.

<#root>

```
kkhapeka@KKHAPEKA-M-F6H2 Downloads %

cat -n  8c3e31be-ca41-43c8-87cb-82a35b0f5213| more


     1  #Cisco DNS and URL intelligence feed: URL Malicious >>>>>name of the category
     2  fadoz.metrs.workers.dev/sell/2641c1ef
     3  oauth-opensea.com
     4  account8133944-complaince.com
```

- باستخدام المسار المنطقي لملفات موجز معلومات الأمان المتطابقة، وأحد الجوانب المهمة لجمع الأدلة هو تنزيل ملفات موجز معلومات الأمان من FTD إلى جهاز محلي يدوي.
- عادةً ما تتم تحديث تلقيمات معلومات الأمان الذكية على فواصل زمنية منتظمة أو يتم تحديث موجز الويب، لا توجد سجلات تغيير على FMC و FTD تشير إلى التغييرات التي تم إجراؤها.
- من خلال تنزيل موجز معلومات الأمان Security Intelligence، يمكنك أخذ لقطة من موجز الويب في هذه اللحظة، ويمكن توفيره لـ BU/TALOS لاحقا.

رارق

يتضمن الحل تحديث موجز معلومات معلومات الأمان وتنفيذ حل بديل مؤقت أثناء انتظار إصلاح البرنامج الدائم.

الخطوة 1: تحديث موجز معلومات معلومات الأمان

قم بتحديث موجز ويب "معلومات الأمان" للحصول على محتوى موجز الويب الذي تم تصحيحه من Talos:

انتقل إلى السياسات > ذكاء الأمان في FMC وقم بتشغيل تحديث موجز ويب يدوي، أو انتظر حتى تكتمل دورة التحديث التلقائي.

الخطوة 2: تنفيذ الحل البديل المؤقت (في حالة إستمرار المشكلة)

إذا إستمرت المشكلة بعد تحديث موجز الويب، فقم بإضافة عناوين URL أو المجالات المتأثرة إلى قائمة "عدم الحظر" كحل بديل مؤقت:

انتقل إلى السياسات > ذكاء الأمان وأضف عناوين IP الخاصة إلى قائمة "عدم الحظر" أسفل علامة التبويب URL.

الخطوة 3: إعادة تمكين فئة URL الضارة

بعد تأكيد تحديث موجز الويب الذي يحل المشكلة، أعد إضافة الفئة "URL Malicious" إلى تكوين معلومات الأمان الذكية:

انتقل إلى السياسات > ذكاء الأمان وأعد تمكين الفئة "URL ضار" ضمن قائمة الحظر.

الخطوة 4: إزالة إدخالات الحل البديل

قم بإزالة مجالات URL/المجالات المتأثرة من قائمة "عدم الحظر" بمجرد تأكيد الإصلاح الدائم وعمله.

الخطوة 5: التحقق من الصحة

تحقق من أن وجهات IP URL الخاصة لم تعد محظورة بواسطة "معلومات الأمان" عن طريق إختبار عناوين URL المتأثرة سابقا ومراقبة أحداث الاتصال في FMC.

السبب

حدثت المشكلة بسبب مشكلة في تحليل محتوى موجز ويب Security Intelligence الذي أثر على سلوك FTD. في موجز معلومات المخابرات الأمنية، كانت هناك عناوين URL بطول يزيد عن 2047 حرفا.

عندما يتجاوز إدخال ما الطول المدعوم، قد يكون جزء من هذه المشكلة بسبب تحميله بشكل غير صحيح كإدخال ضار منفصل، مما قد يؤدي إلى حظر حركة المرور غير المرتبطة. يتم تتبع هذا السلوك تحت معرف خطأ Cisco: CSCww11335. تم حل المشكلة من خلال التغييرات التصحيحية التي قام بها فريق Talos إلى محتوى موجز الويب، مع تخطيط إصلاح برنامج دائم لإصدار لاحق لإضافة حواجز حماية تمنع التكرارات المستقبلية.

المحتوى ذي الصلة

- معرف الخطأ من Cisco: CSCww11335
- الدعم الفني والتنزيلات من 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).