أستكشاف أخطاء نظام قناة SLIC وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء نظام تحليلات الشبكة الآمنة (SNA) "Slic Channel Down" وإصلاحها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بوجود معرفة SNA الأساسية لديك.

SLIC تعني "مركز معلومات مختبرات Stealthwatch"

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الإجراء

يتم تشغيل التنبيه "SLIC Channel Down" عندما لا يتمكن مدير SNA من الحصول على تحديثات موجز الويب من خوادم معلومات التهديد، التي كانت سابقا SLIC. لفهم الأسباب التي أدت إلى مقاطعة تحديثات موجز الويب بشكل أفضل، قم بالمتابعة على النحو التالي:

1. قم بالاتصال بمدير SNA عبر SSH وسجل الدخول باستخدام **root** بيانات الاعتماد.
2. تحليل **/lancope/var/smc/log/smc-core.log** ابحث عن سجلات النوع **SlicFeedGetter**.

بمجرد العثور على السجلات ذات الصلة، انتقل إلى القسم التالي نظرا لوجود حالات متعددة يمكن أن تتسبب في تشغيل هذا التنبيه.

سجلات الأخطاء الشائعة

أكثر سجلات الأخطاء شيوعا التي تم رؤيتها في **smc-core.log** متعلقة بالإذن الخاص بقناة السليك أسفل:

انتهت مهلة الاتصال

```
<#root>

2023-01-03 22:43:28,533 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-03 22:43:28,592 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-03 22:43:28,592 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=2019
2023-01-03 22:45:39,604

ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.


org.apache.http.conn.HttpHostConnectException: Connect to lancope.flexnetoperations.com:443 [lancope.fle
```

تعذر العثور على مسار شهادة صالح للهدف المطلوب

```
<#root>

2023-01-04 00:27:50,497 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-04 00:27:50,502 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-04 00:27:50,502 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=2019
2023-01-04 00:27:51,239

ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.


javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPa
```

فشلت المصافحة

<#root>

```
2023-01-02 20:00:49,427 INFO [SlicFeedGetter] Performing request to get Threat Feed update file.
2023-01-02 20:00:49,433 INFO [SlicFeedGetter] Threat Feed Host 'lancope.flexnetoperations.com' resolves
2023-01-02 20:00:49,433 INFO [SlicFeedGetter] Threat Feed URL: /control/lncp/LancopeDownload?token=2019
```

2023-01-02 20:00:50,227 ERROR [SlicFeedGetter] Getting Threat Feed update failed with exception.

javax.net.ssl.SSLHandshakeException: Handshake failed

خطوات التنفيذ

يمكن مقاطعة تحديثات موجز ويب إستخبارات التهديد بسبب ظروف مختلفة. قم بإجراء خطوات التحقق التالية للتأكد من أن إدارة SNA تفي بالمتطلبات.

الخطوة 1. التحقق من حالة الترخيص الذكي

انتقل إلى **Central Management** > **Smart Licensing** وضمان أن حالة ترخيص موجز التهديد هي **Authorized**.

الخطوة 2. التحقق من تحليل نظام اسم المجال (DNS)

تأكد من قدرة إدارة SNA بنجاح على حل عنوان IP لـ **lancope.flexnetoperations.com** and esdhttp.flexnetoperations.com

الخطوة 3. التحقق من الاتصال بخوادم موجز معلومات التهديد

تأكد من أن مدير SNA لديه حق الوصول إلى الإنترنت وأن الاتصال بخوادم معلومات التهديد المدرجة التالية مسموح به:

الوجهة	المصدر	المنفذ والبروتوكول
esdhttp.flexnetoperations.com lancope.flexnetoperations.com	مدير SNA	بروتوكول TCP/443

ملاحظة: إذا لم يسمح لمدير SNA بالوصول المباشر إلى الإنترنت، فيرجى التأكد من وجود تكوين الوكيل للوصول إلى الإنترنت.

الخطوة 4. تعطيل فحص/فك تشفير طبقة مأخذ التوصيل الآمنة (SSL)

الاخطاء الثانيه والثالثه الموضحه في **Common Error Logs** يمكن أن يحدث القسم عندما ال تتلقى إدارة SNA شهادة الهوية الصحيحة أو سلسلة الثقة الصحيحة المستخدمة من قبل خوادم زجم معلومات معلومات التهديد. ولمنع ذلك، تأكد من عدم إجراء فحص/فك تشفير SSL عبر شبكتك (بواسطة جدران الحماية القوية أو الخوادم الوكيلة) للاتصالات بين مدير SNA وخوادم معلومات التهديد المدرجة في **Verify Connectivity to the Threat Intelligence Feed Servers** قسم.

إذا لم تكن متأكدا من تنفيذ فحص/فك تشفير SSL في شبكتك، فيمكنك تجميع التقاط حزمة بين عنوان IP الخاص بإدارة SNA وعنوان IP الخاص بخوادم ذكاء التهديدات وتحليل الالتقاط للتحقق من الشهادة المستلمة. للقيام بذلك، قم بأداء ما يلي:

1. اتصل بمدير SNA بواسطة SSH وسجل الدخول باستخدام **root** بيانات الاعتماد.
2. قم بتشغيل أحد الأمرين المدرجين بعد ذلك (يعتمد الأمر الذي سيتم تشغيله على ما إذا كان مدير SNA يستخدم خادم وكيل للوصول إلى الإنترنت أم ال):

```
tcpdump -w /lancope/var/tcpdump/slic_issue.pcap -nli eth0 host 64.14.29.85
tcpdump -w /lancope/var/tcpdump/slic_issue2.pcap -nli eth0 host [IP address of Proxy Server]
```

3. دع عملية الالتقاط تستمر لمدة دقيقتين إلى 3 دقائق ثم أوقفها.
4. نقل الملف الذي تم إنشاؤه من إدارة SNA للتحليل. ويمكن تحقيق ذلك باستخدام بروتوكول النسخ الآمن (SCP).

عيوب ذات صلة

هناك عيب واحد معروف يمكن أن يؤثر على الاتصال بالخوادم SLIC:

- يمكن أن يتوقف اتصال SMC الأساسي ويفشل إذا تم حظر منفذ الوجهة 80. راجع معرف تصحيح الأخطاء من Cisco CSCwe08331

معلومات ذات صلة

- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات اتصال دعم Cisco في جميع أنحاء العالم.
- يمكنك أيضا زيارة مجتمع تحليلات الأمان من Cisco هنا.
- الدعم التقني والمستندات - Cisco Systems

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).