أستكشاف أخطاء نتائج فحص أمان سلسلة دعن بعد التواجد نظام الصإو SUDI شهادات

المحتويات

مسألة

تقوم عمليات المسح الضوئي لنقاط الضعف الأمنية بتعليم النتائج المتعلقة بشهادات SSL/TLS على نقاط النهاية لبرنامج ترميز الفيديو Cisco TelePresence، والتي تقوم تحديدا بالإبلاغ عن سلسلة شهادات غير موثوق بها على منافذ TCP رقم 4053 و 4060 و 4062. يقوم الماسح الضوئي لتحديد الثغرات بعرض برنامج الترميز شهادة CS-Room صادرة عن ACT2 SUDI CA (المنظمة: Cisco) في Cisco Root CA مع انتهاء سلسلة الشهادات في 2048. يقوم نظام المسح الضوئي للأمان بالإعلام عن هذا الأمر على أنه سلسلة شهادات غير موثوق بها لا تفي بمتطلبات الأمان للمؤسسة.

تشمل النتائج المحددة التي تم الإبلاغ عنها من خلال عمليات الفحص الأمني ما يلي:

- كشف الشهادة الموقع ذاتيا
- سلسلة شهادات غير موثوق بها
- مخاوف خوارزمية التجزئة الضعيفة
- تحذيرات انتهاء صلاحية الشهادة

البيئة

- نقاط نهاية ترميز الفيديو Cisco TelePresence
- أجهزة Webex Desk Series مع التسجيل المحلي
- نقاط النهاية بشرائح ACT2 SUDI (معرف الجهاز الفريد الآمن)
- مشاكل سلسلة الشهادات الخاصة بمسح البنية الأساسية لعلامات تمييز الثغرات الأمنية

- شهادات SUDI التي تقدم على المنافذ TCP أرقام 4062 و 4060 و 4053

قرار

تكون شهادات SUDI على نقاط نهاية Cisco TelePresence مضمنة، أو شهادات ثابتة لا يمكن تعديلها، أو إعادة توليدها، أو حذفها بطريقة مدعومة. تعد هذه الشهادات جزءا من تنفيذ تقنيات Cisco الجديرة بالثقة وتخدم وظائف أمان معينة.

فهم سلوك شهادة SUDI

يختلف سلوك الشهادة حسب تكوين المنفذ والنظام:

- المنفذ 4053 (خدمة الاقتران): يستخدم شهادات SUDI عندما يحتوي النظام على شريحة الأنظمة التي لا تحتوي على شريحة ACT2. لا تستخدم الشهادات المخصصة إلا على نقاط النهاية الأقدم (ACT2).
- منفذ 4047: يستخدم شهادات خيارها العملاء للاتصال بين لوحات اللمس والشفرات.

موقع الشهادة وتفاصيلها

توجد شهادات SUDI في مخزن شهادات الجهاز:

```
device:~] $ cd /etc/cacerts_sudi
  device:/etc/cacerts_sudi] $ ls
0763c37d.0              9426d327.0              mic-cbasrcarsa4k2099.pem
29cf4e89.0              a094437b.0              mic-cmca.pem
36087b08.0              b35c8d6c.0              mic-cmca2.pem
417aa245.0              cmca2.pem               mic-cmca3.pem
771a09b9.0              crca2048.pem            mic-cmca4.pem
89087fe6.0              crca2099.pem            mic-crcam2.pem
90359431.0              mic-cbarc2099.pem       mic-harsa-ca.pem
```

تفاصيل شهادة ACT2 SUDI CA:

```
CN = ACT2 SUDI CA
```

O = Cisco
Valid From: Thursday, June 30, 2011 11:26:57 PM
Valid To: Tuesday, May 15, 2029 1:55:42 AM

الإجراءات الموصى بها

الخطوة 1: مراجعة غرض شهادة SUDI وتطبيق الأمان

شهادة SUDI غير موقعة ذاتيا ولكنها موقعة من قبل Cisco Manufacturing CA. إنه بمثابة بيانات اعتماد هوية ثابتة:

- الاحتفاظ بمعرف المنتج والرقم التسلسلي
- يوفر هوية غير قابلة للتغيير للتكوين والأمان ومراجعة الحسابات والإدارة
- مشفر مرتبط بشريحة وحدة إرساء الثقة
- يجعل الاستنساخ أو الانتحال شبه مستحيل

الخطوة 2: العمل مع فريق الأمن لاستباعاد نتائج شهادة SUDI

وبما أن شهادات SUDI لا يمكن تعديلها وتخدم وظائف أمنية مشروعة، فإن النهج الموصى به هو:

- تكوين أدوات مسح الأمان لاستباعاد نتائج سلسلة شهادات SUDI للخدمات المتأثرة
- توثيق مبررات الأعمال للاستثناء استنادا إلى تنفيذ تقنيات Cisco الموثوق بها
- ركز فحص الأمان على الشهادات القابلة للتهيئة من قبل العميل على المنافذ الأخرى إذا لزم الأمر

الخطوة 3: تحديثات الشهادات من خلال ترقيات البرامج

تحدث تحديثات الشهادات في المخزن الموثوق به تلقائيا عند ترقية النظام إلى إصدارات برامج أحدث. وهذا يضمن الحفاظ على صلاحية الشهادة مع مرور الوقت.

قيود مهمة

تنطبق هذه القيود على شهادات SUDI:

- لا يمكن تعديله أو إعادة توليده أو حذفه
- يحدث إعادة الإنشاء التلقائي إذا تم حذف الشهادات وإعادة تشغيل الجهاز
- لا توجد طريقة معتمدة لتعيين شهادات قابلة للتكوين إلى خدمات النهاية الخلفية هذه
- لا يمكن إستبدال الشهادة نظرا للطبيعة الثابتة لتطبيق Trust Anchor

السبب

يتم إطلاق نتائج مسح الأمان بوساطة وجود شهادات SUDI (معرف الجهاز الفريد الآمن) من Cisco، والتي هي شهادات تصنيع مضمنة تتسلسل إلى Cisco Root CA 2048. تعد هذه الشهادات جزءا من تنفيذ تقنيات Cisco الجديرة بالثقة وتم تصميمها لتكون ثابتة لأغراض الأمان. لا يتم التعرف على الشهادات كشهادات موثوق بها من قبل أدوات الفحص الأمني للمؤسسة لأنها تنتهي في مرجع شهادات Cisco الرئيسي بدلا من مرجع مصدق مصدق خاص بمؤسسة. هذا سلوك متوقع للأجهزة التي تدعم SUDI ويمثل ميزة تصميم بدلا من ضعف أمني.

المحتوى ذي الصلة

- [وقة بيانات التقنيات الجديرة بالثقة من Cisco](#)
- [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).