الأسئلة المتداولة Cisco TAC التقنية ل Cisco IOS XE Software Web UI Privilege Escalation Vulnerability - CVE-2023-20198

المحتويات

المقدمة

يمثل هذا المستند الأسئلة المتداولة التقنية الخاصة بمركز المساعدة التقنية ل Cisco IOS XE Software Web UI الخاصة بمجموعة التصعيد الخاصة بامتياز Cisco IOS XE. تتوفر تفاصيل إضافية في إشعار الأمان لنقاط الضعف مدونة Cisco Talos.

نظرة عامة

يوضح هذا المستند تأثيرات تعطيل أوامر ip http server أو ip http secure-server وما هي الوظائف الأخرى التي تتأثر من خلال القيام بذلك. وبالإضافة إلى ذلك، فإنه يقدم أمثلة على كيفية تكوين قوائم الوصول الموضحة في الإرشادات للحد من الوصول إلى شبكة webui في حالة عدم قدرتك على تعطيل الميزات بالكامل.

1. هل يتأثر منتجي؟

تتأثر فقط المنتجات التي تشغل برنامج Cisco IOS XE بالإصدارات 16.x والإصدارات الأعلى. لا تتأثر منتجات Nexus و ACI أو أجهزة IOS التقليدية و IOS XR وجدران الحماية (ASA/FTD) و ISE. في حالة Identity Services Engine، قد يكون هناك تأثيرات أخرى لتعطيل خادم HTTP/HTTPS. الرجاء مراجعة قسم ISE.

2. كيف يمكنني تحديد ما إذا كان منتجي يعمل بنظام Cisco IOS XE؟

قم بتنفيذ الأمر show version من واجهة سطر الأوامر (CLI) وستر ى نوع البرنامج مثل هذا:

switch#show version

برنامج Cisco IOS XE، الإصدار 17.09.03

برنامج Cisco IOS [Curelated]، برنامج C9800-CL (C9800-CL-K9_IOSXE)، الإصدار 17.9.3، برنامج الإصدار (FC6)

الدعم التقني: http://www.cisco.com/techsupport

حقوق النشر (c) 1986-2023 بواسطة Cisco Systems، Inc.

Tue 14-MAR-23 18:12 حسب MCPRE

برنامج Cisco IOS-XE، حقوق النشر (c) 2005-2023 بواسطة Cisco Systems، Inc.

جميع الحقوق محفوظة. يتم ترخيص بعض مكونات برنامج Cisco IOS-XE بموجب الترخيص العام GNU ("GPL") الإصدار 2.0. كود البرنامج المرخص به بموجب GPL الإصدار 2.0 وه برنامج مجاني يأتي بدون ضمان على الإطلاق. يمكنك إعادة توزيع و/أو تعديل رمز GPL هذا طبقا لبنود GPL الإصدار 2. 0. لمزيد من التفاصيل، راجع الوثائق أو ملف "إشعار الترخيص" المرفق ببرنامج IOS-XE أو عنوان URL القابل للتطبيق والموزود في النشرة المرفقة ببرنامج IOS-XE.

والتأثر بهذا الضعف إلا إصدارات البرامج 16.x والإصدارات الأحدث. مثال إصدارات البرامج المتأثرة هي:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

أمثلة إصدارات IOS XE التي لا تتأثر:

3,17,4 ثانية

3,11,7 س ا

15,6-1,s 4

15,2-7,E7

3. أنا أستخدم حالات إعادة توجيه إستخدام محرك خدمات الهوية (ISE) والي يمكنني تعطيل خوادم HTTP/HTTPS. ماذا يمكنني أن أفعل؟

سيؤدي تعطيل خادم ip http و ip http secure-server إلى منع حالات الاستخدام مثل التالية من العمل:

- التنميط المستند إلى مستشعر الجهاز
- إعادة توجيه الوضع والاكتشاف
- إعادة توجيه الضيف
- ضم باي دو
- ضم MDM

في أجهزة IOS-XE التي لا تتطلب الوصول إلى Webui، يوصى باستخدام الأوامر التالية لمنع الوصول إلى Webui مع الاستمرار في السماح بحالات إعادة توجيه إستخدام ISE:

- ip http active-session-modules none
- ip http secure-active-session-modules none

إذا كانت هناك حاجة إلى الوصول إلى واجهة المستخدم (WEBUI)، مثل إستخدام وحدات التحكم Catalyst 9800، يمكن تقييد الوصول إلى واجهة المستخدم (WEBUI) باستخدام قوائم التحكم في الوصول من فئة HTTP: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

لا تزال قوائم التحكم في الوصول من فئة الوصول إلى HTTP تسمح بحالات إعادة توجيه إستخدام ISE كي تعمل.

4. أنا أستخدم C9800 السلكي lan جهاز تحكم (WLC) والي يستطيع أعجزت ال http/http نادل. ماذا يمكنني أن أفعل؟

A4. سيؤدي تعطيل ip http server و ip http secure-server إلى كسر حالات الاستخدام التالية:
- الوصول إلى واجهة مستخدم ويب WLC. هذا صحيح سواء كانت واجهة الإدارة اللاسلكية أو أي SVI آخر يتم إستخدامه للوصول إلى واجهة المستخدم الرسومية (WMI) أو منفذ الخدمة أو (GUI) ل WebAdmin.
- سيفشل معالج إعداد اليوم 0.
- مصادقة الويب - وصول الضيف ما إذا كانت الصفحة الداخلية الخاصة بوحدة التحكم

في الشبكة المحلية اللاسلكية (WLC) ومصادقة الويب المخصصة ومصادقة الويب المحلية والمصادقة المركزية للويب ستتوقف عن إعادة التوجيه

- في C9800-CL، سيفشل إنشاء الشهادة الموقع ذاتيا
- الوصول إلى RESTCONF
- S3 و CloudWatch
- إستضافة تطبيق IOx على نقاط الوصول اللاسلكية

لمتابعة إستخدام هذه الخدمات، ستحتاج إلى القيام بالخطوات التالية:

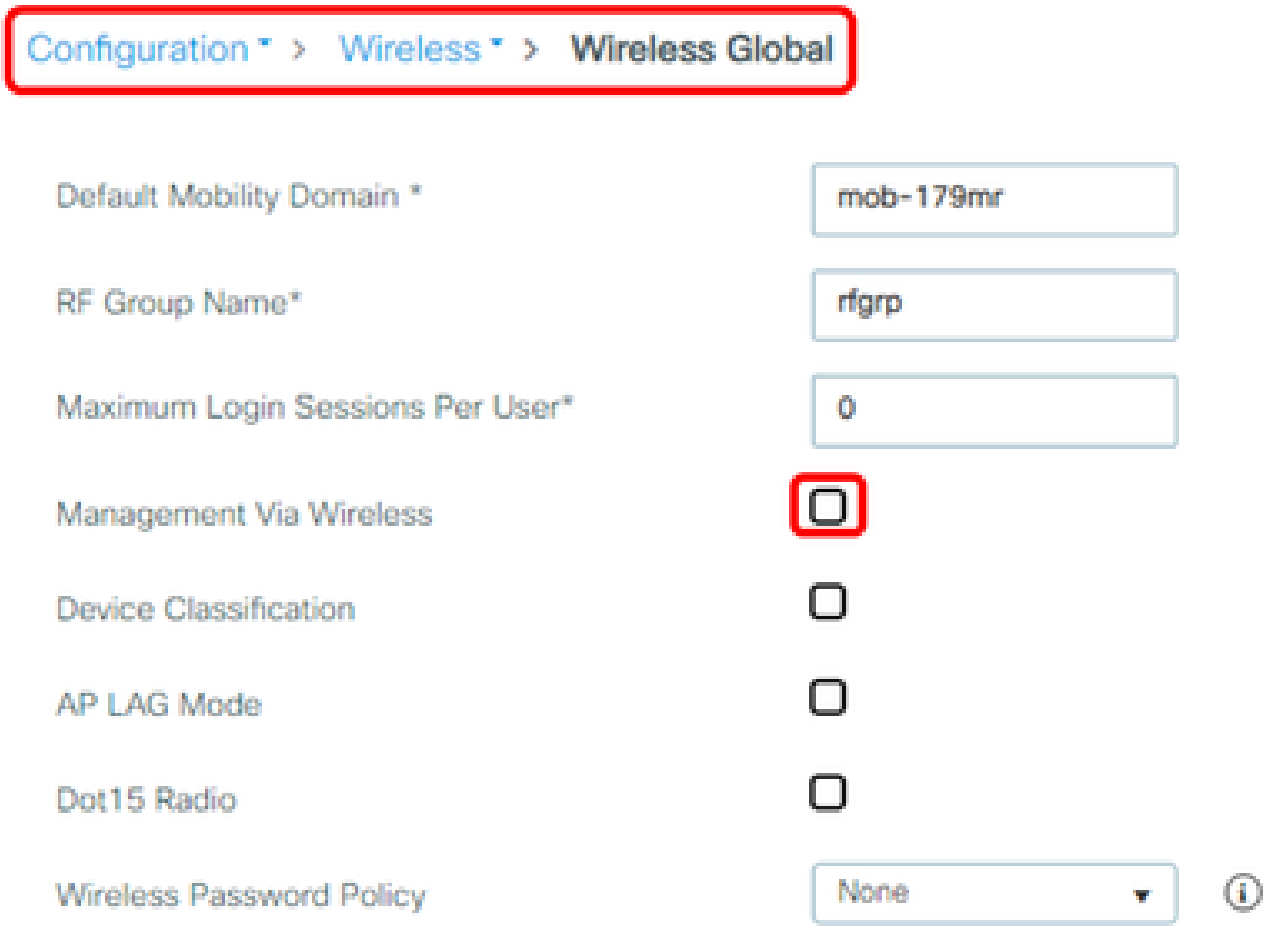
(1) الحفاظ على تمكين بروتوكول HTTP/HTTPS

(2) أستخدم قائمة تحكم في الوصول (ACL) للحد من الوصول إلى خادم الويب C9800 WLC، فقط إلى الشبكات الفرعية / العناوين الموثوق بها.
يمكن العثور على تفاصيل حول تكوين قائمة الوصول:
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html.

ملاحظة:
1 - لا تكون الشركات المحلية اللاسلكية الصغيرة في نظام AireOS
2. تتأثر كافة تصميمات C9800 (C9800-80، C9800-40، C9800-L، C9800-CL) بما في ذلك الشبكات اللاسلكية المضمنة على نقطة الوصول (EWC-AP) والمحول اللاسلكي المضمن على المحول (EWC-SW)
3. تقوم قائمة التحكم في الوصول ل HTTP بحظر الوصول إلى خادم HTTP على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) C9800 فقط. لن يؤثر ذلك على وصول ضيف WebAuth سواء كان ذلك باستخدام الصفحة الداخلية ل WLC أو صفحة مصادقة ويب مخصصة أو مصادقة ويب محلية أو مصادقة ويب المركزية
4. تؤثر قائمة التحكم في الوصول ل HTTP أيضا على التحكم في CAPWAP أو حركة مرور البيانات.
5. تأكد من عدم السماح بالشبكات غير الموثوق بها مثل الضيف في قائمة التحكم في الوصول (ACL) ل HTTP.

إختياري، إذا كنت تريد منع عملائك اللاسلكيين من الوصول إلى واجهة المستخدم الرسومية (GUI) ل WebAdmin بشكل كامل، فتأكد من تعطيل "الإدارة عبر الشبكة اللاسلكية".

GUI:



CLI:

```
C9800(config)#no wireless mgmt-via-wireless
C9800(config)#exit
```

5. في تحذير الأمان الذي يذكره هناك قواعد شخير للكشف عن هذه الهشاشة وحظرها. كيف يمكنني تأكيد تثبيت هذه القواعد والعمل على "برنامج الإرسال فائق السرعة (FTD)" الخاص بي؟

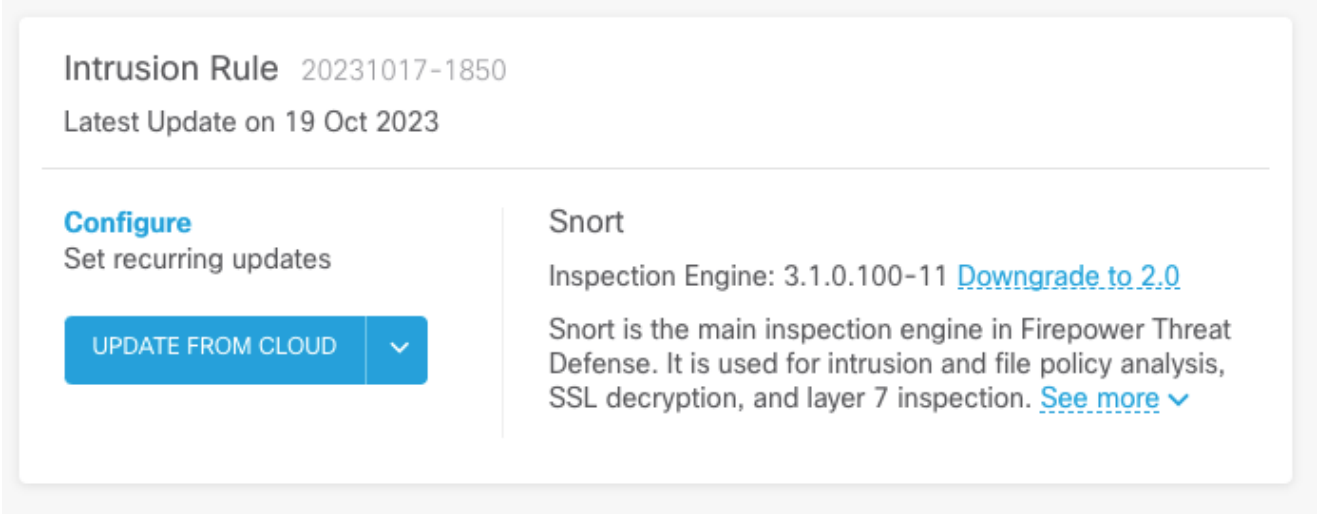
للتأكد من تثبيت قواعد التطفل على جهازك، تحقق للتأكد من وجود LSP 20231014-1509 أو SRU-2023-10-14-001 لديك. التحقق مهم إذا كان هذا مثبتا بشكل مختلف على الأجهزة المدارة من FDM و FMC:

أ. تأكد من تثبيت القواعد:

FDM

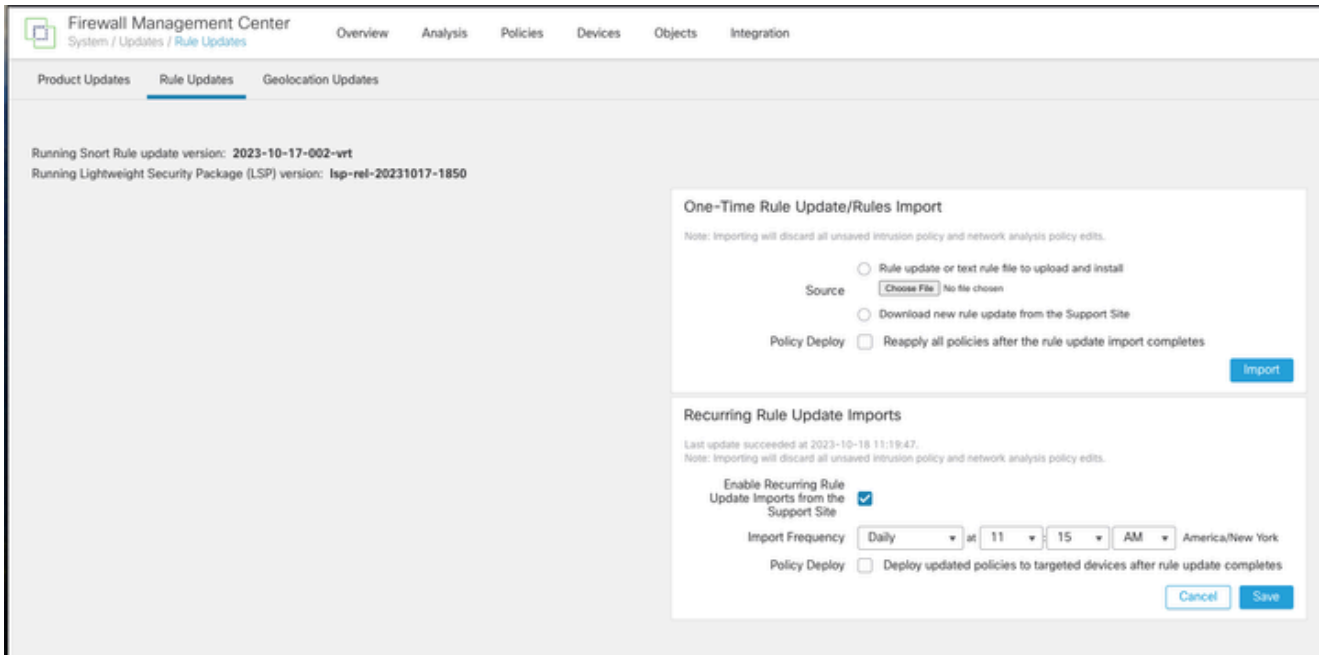
1. انتقل إلى الجهاز > التحديثات (عرض التكوين)

2. تحقق من قاعدة التطفل وتأكد من أنها 20231014-1509 أو أحدث



FMC

1. انتقل إلى النظام > التحديثات > تحديثات القواعد
2. تحقق من تشغيل تحديث قاعدة الشخيرات وتشغيل حزمة الأمان Lightweight (LSP) وتأكد من أنهم يشغلون LSP 20231014-1509 أو SRU-2023-10-14-001 أو أعلى.



ب. تأكد من القواعد الممكنة في سياسة التطفل الخاصة بك

إذا كانت نهج التسلل قائمة على نهج Talos المدمجة (الاتصال عبر الأمان والأمان عبر الاتصال والأمان المتوازن والاتصال) فسيتم تمكين هذه القواعد وتعيينها للإسقاط بشكل افتراضي.

إذا لم تكن تقوم على أحد السياسات المدمجة في Talos. ستحتاج إلى تمكين تعيين إجراءات القاعدة يدويا لهذه القواعد في نهج التسلل. للقيام بذلك، يرجى مراجعة الوثائق التالية:

نورت 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-

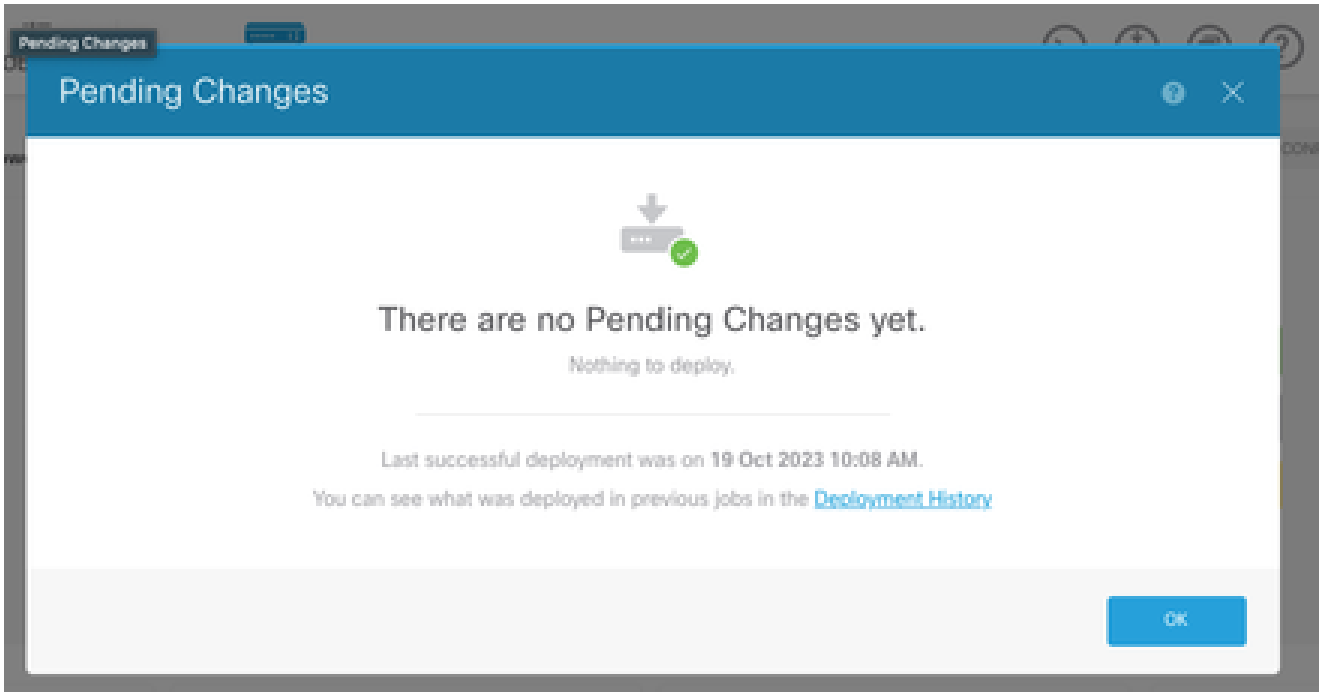
center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

نورت 2: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/intrusion-tuning-rules.html#ID-2237-00000683

ج. تأكد من نشر سياسات التبديل داخل الشاشة (IPS) على أجهزة FTD لديك:

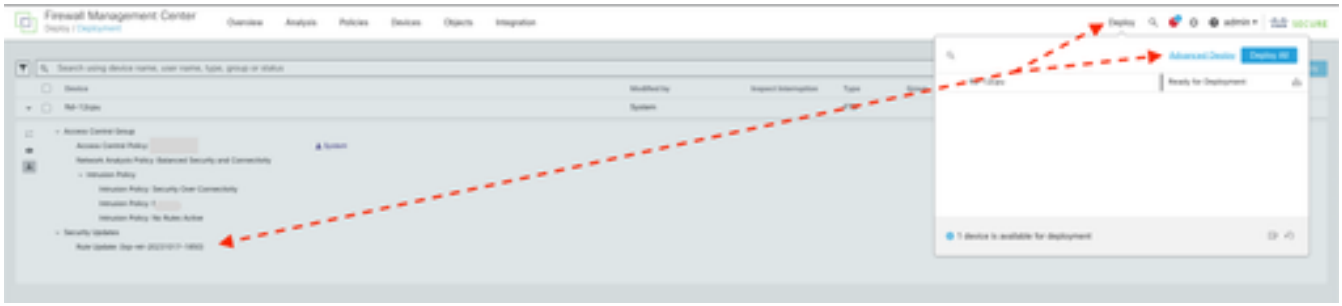
FDM

1. انقر على رمز النشر
2. التأكد من عدم وجود تغييرات معلقة تتعلق بوحدة sru/LSP



FMC

1. انقر فوق نشر > نشر متقدم
2. تأكد من عدم وجود عمليات نشر معلقة تتعلق بوحدة الخدمة SRU/LSP



6. لدي عنصر حدود موحد (CUBE) من Cisco يشغل برنامج Cisco IOS XE. هل يمكنني تعطيل خادم http/https؟

لا تستخدم معظم عمليات نشر المكعب خدمة HTTP/HTTPS المضمنة مع IOS XE ولن يؤثر تعطيلها على الوظائف. إذا كنت تستخدم ميزة البحث عن الوسائط المستندة إلى XMF، فستحتاج عندئذ إلى تكوين قائمة وصول وتقييد الوصول إلى خدمة HTTP لتضمين الأجهزة المضيفة الموثوقة (عملاء CUCM/الطرف الثالث) فقط. يمكنك عرض مثال تكوين هنا.

7. لدي مدير إتصالات موحد Express (CME) من Cisco يشغل برنامج Cisco IOS XE. هل يمكنني تعطيل خادم http/https؟

يستخدم حل CME خدمات HTTP إلى دليل المستخدم والخدمات الإضافية لهواتف IP المسجلة. سيؤدي تعطيل الخدمة إلى فشل هذه الوظيفة. ستحتاج إلى تكوين قائمة وصول وتقييد الوصول إلى خدمة HTTP لتضمين الشبكة الفرعية لشبكة IP Phone فقط. يمكنك عرض مثال تكوين هنا.

8. إذا قمت بتعطيل خادم http/https، فهل سيؤثر هذا على قدرتي على إدارة أجهزتي باستخدام مركز بنية الشبكة الرقمية (DNA) من Cisco؟

لن يؤثر تعطيل خادم HTTP/HTTPS على وظائف إدارة الأجهزة أو إمكانية الوصول للأجهزة التي تتم إدارتها باستخدام مركز بنية الشبكة الرقمية (DNA) من Cisco، بما في ذلك تلك الموجودة في بيئات SDA (الوصول المعرف بالبرامج). سيكون لتعطيل خادم HTTP/HTTPS تأثير على ميزة إستضافة التطبيقات، وأي تطبيقات من إنتاج جهات خارجية يتم إستخدامها داخل بيئة إستضافة التطبيقات لمركز بنية الشبكة الرقمية من Cisco. قد تعتمد هذه التطبيقات التابعة لجهات خارجية على خادم HTTP/HTTPS للاتصال والوظائف.

9. هل سيكون هناك تأثير على الترخيص الذكي إذا قمنا

بتعطيل خادم HTTP/HTTPS على الجهاز؟

وبشكل عام، يستخدم "الترخيص الذكي" وظائف عميل HTTPS، ومن ثم لا يؤثر تعطيل ميزة خادم HTTP(s) على عمليات الترخيص الذكية. والسيناريو الوحيد الذي يؤدي إلى تعطيل الاتصال الذكي بالترخيص هو عندما يتم إستخدام تطبيق CSLU الخارجي أو SSM على PREM وتكوينه باستخدام RESTCONF لاسترداد تقارير RUM من الأجهزة.

10. هل يمكن لممثل التهديد إستغلال الثغرات الأمنية وإنشاء مستخدم محلي حتى إذا كان المصادقة والتفويض والمحاسبة (AAA) في موضعه؟

نعم، نحن نعتقد أن ممثل التهديد يمكن أن يستغل هذه الثغرة لإنشاء مستخدم محلي بغض النظر عن طريقة المصادقة التي تستخدمها. يرجى ملاحظة أن بيانات الاعتماد ستكون محلية بالنسبة للجهاز المستغل وليست موجودة في نظام AAA.

11. ما هي الاستجابة "curl" إذا كنت أستخدم الموجه الخاص بي كخادم CA وتم تكوين قائمة التحكم في الوصول لحظر IP الخاص بالجهاز HTTP/S بالفعل؟

تم منع الاستجابة "curl" بنسبة 403 كما هو موضح أدناه:

(base) سطح المكتب ~ ٪ curl http://<device ip>

<html>

<head><title>403 ممنوع</title></head>

<body bgcolor="white">

<h1>403 ممنوع</h1>

<hr> nginx

</body>

</html>

12. أين يمكنني العثور على المعلومات المتعلقة بإصلاح البرامج أو توفر وحدات صيانة البرامج (SMU)؟

يرجى زيارة صفحة الثغرات الخاصة بتصعيد امتياز واجهة مستخدم الويب لبرنامج Cisco IOS XE للحصول على مزيد من المعلومات.

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).