تخفيف انتحال بروتوكول CVE-2024-3596 لنصف قطر الانفجار

المحتويات

المقدمة

في 7 يوليو/تموز 2024، كشف باحثو الأمن عن نقاط الضعف التالية في بروتوكول RADIUS: CVE-2024-3596: بروتوكول RADIUS بموجب RFC 2865 قابل لهجمات تزييف من قبل مهاجم في المسار يمكنه تعديل أي إستجابة صالحة (قبول الوصول أو رفض الوصول أو تحدي الوصول) لأي إستجابة أخرى باستخدام هجوم تصادم البادئة المختارة ضد توقيع مصدق إستجابة MD5. وقد نشرت ورقة تفصل النتائج التي توصلت إليها على الموقع https://www.blastradius.fail/pdf/radius.pdf، وهي تبين أن هناك عملية تزوير ناجحة في الاستجابة للتدفقات التي لا تستخدم سمة مصدق الرسائل.

للحصول على قائمة محدثة بمنتجات Cisco التي تأثرت بنقاط الضعف هذه والإصدارات التي تحتوي على إصلاحات، يرجى زيارة: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. تغطي هذه المقالة تقنيات التخفيف العامة بالإضافة إلى كيفية تطبيقها على بعض منتجات Cisco، ولكن ليس جميع منتجات Cisco، يجب الرجوع إلى وثائق المنتجات الفردية للحصول على تفاصيل. كخادم رائد ل Cisco RADIUS، ستتم تغطية محرك خدمة الهوية بمزيد من التفاصيل.

الخلفية

يستغل هذا الهجوم هجوم بادئة MD5 المختارة باستخدام التصادمات في MD5، والتي تسمح للمهاجم بإضافة بيانات إضافية إلى حزمة إستجابة RADIUS أثناء تعديل السمات الموجودة لحزمة الاستجابة. وقد تمثل المثال الذي تم توضيحه في القدرة على تغيير رفض الوصول إلى RADIUS إلى قبول وصول RADIUS. وهذا ممكن لأن RADIUS لا يتضمن بشكل افتراضي تجزئة لكل السمات في الحزمة. لا يقوم RFC 2869 بإضافة سمة مصدق الرسائل ولكنها حالياً مطلوبة للتضمين عند إستخدام بروتوكولات EAP، مما يعني أن وصف الهجوم في CVE-2024-3596 ممكن مقابل أي تبادل غير EAP حيث لا يتضمن عميل RADIUS (NAD) سمة مصدق الرسائل.

تخفيف

مصدق الرسائل

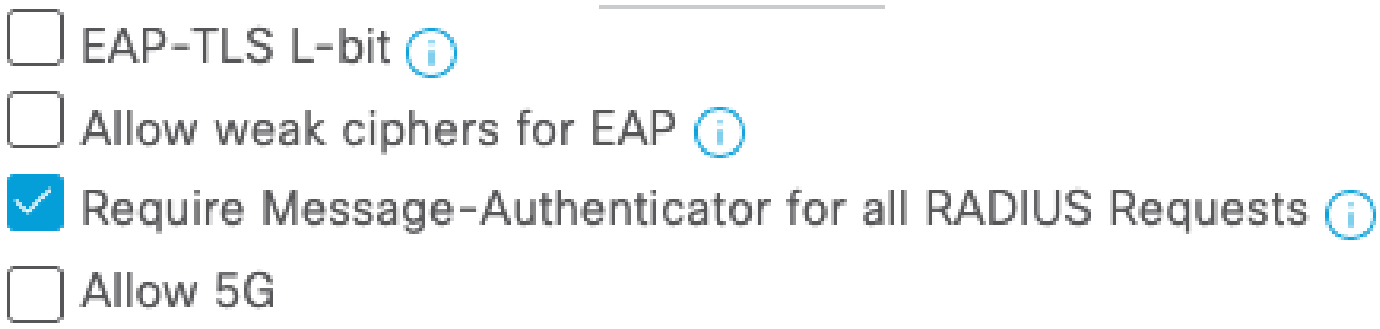
1) يجب أن يتضمن عميل RADIUS سمة مصدق الرسائل.

عندما يتضمن جهاز الوصول إلى الشبكة (NAD) سمة مصدق الرسائل في طلب الوصول،

سيتضمن محرك خدمات الهوية مصدق الرسائل في الحزمة الناتجة قبول الوصول أو اعتراض الوصول أو رفض الوصول في جميع الإصدارات.

2) يجب أن يفرض خادم RADIUS تلقي سمة مصدق الرسائل.

والكيفية مجرد تضمين مصدق الرسائل في طلب الوصول لأن الهجوم يجعل من الممكن أن يجرد مصدق الرسائل من طلب الوصول قبل أن تتم إعادة توجيهه إلى خادم RADIUS. كما يجب أن يتطلب خادم RADIUS أن يتضمن NAD مصدق الرسائل في طلب الوصول. وهذا الأمر ليس افتراضيا على Identity Services Engine (محرك خدمات الهوية) ولكن يمكن تمكينه على مستوى البروتوكولات المسموح بها، والذي يتم تطبيقه على مستوى مجموعة النهج. الخيار ضمن تكوين البروتوكولات المسموح بها هو "طلب مصدق الرسالة" لجميع طلبات RADIUS:



خيار البروتوكولات المسموح بها في محرك خدمات الهوية

عمليات المصادقة التي تطابق مجموعة نهج حيث يتطلب تكوين البروتوكولات المسموح بها مصادقة الرسائل، ولكن في حالة عدم إحتواء طلب الوصول على سمة مصدق الرسائل سيتم إسقاطها من قبل ISE:

Event	5405 RADIUS Request dropped
Failure Reason	11057 Message-Authenticator attribute is missing in RADIUS Access-Request

من المهم التحقق مما إذا كان NAD يرسل مصدقا للرسائل قبل أن يكون مطلوبا بواسطة خادم RADIUS لأن هذه ليست سمة تم التفاوض عليها، فمن حق NAD إرسالها أم بشكل افتراضي أو أن يتم تكوينه لإرسالها. الى يعد مصدق الرسائل إحدى السمات التي تم الإبلاغ عنها بواسطة ISE، ويعد التقاط الحزمة أفضل طريقة لتحديد ما إذا كانت حالة NAD/User تتضمن مصدق الرسائل. قام ISE بإنشاء وظيفة التقاط الحزم ضمن Operations -> Diagnostic Tools -> General Tools -> TCP Dump. تذكر أن حالات أستكشاف الأخطاء وإصلاحها الاستخدام المختلفة من نفس NAD يمكن أن تتضمن أو لا تتضمن مصدق الرسائل.

فيما يلي التقاط مثال ل Access-Request يتضمن سمة مصدق الرسائل:

```
No.  | Time          | Source          | Destination     | Protocol | Length | Info
   1 | 11:27:30.116244 | 14.0.65.75      | 172.18.124.20   | RADIUS   |    306 | Access-Request id=11
   2 | 11:27:30.184821 | 172.18.124.20   | 14.0.65.75      | RADIUS   |    187 | Access-Accept id=11
   3 | 11:27:31.242718 | 14.0.65.75      | 172.18.124.20   | RADIUS   |    313 | Accounting-Request id=8
   4 | 11:27:31.258999 | 172.18.124.20   | 14.0.65.75      | RADIUS   |     62 | Accounting-Response id=8

> Frame 1: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits)
> Ethernet II, Src: Cisco_4a:81:02 (6c:b2:ae:4a:81:02), Dst: VMware_c9:84:88 (00:0c:29:c9:84:88)
> Internet Protocol Version 4, Src: 14.0.65.75, Dst: 172.18.124.20
> User Datagram Protocol, Src Port: 1645, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xb (11)
    Length: 264
    Authenticator: a8f87e2a6e40c7c87465456fae0c2b79
    [The response to this request is in frame 2]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=14 val=5c838ff850d8
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1500
    > AVP: t=Called-Station-Id(30) l=19 val=34-A8-4E-DB-07-04
    > AVP: t=Calling-Station-Id(31) l=19 val=5C-83-8F-F8-50-D8
    > AVP: t=Message-Authenticator(80) l=18 val=f2116042ddcd47db45053dd0e76212de
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=192.168.16.127
    > AVP: t=NAS-IP-Address(4) l=6 val=14.0.65.75
    > AVP: t=NAS-Port-Id(87) l=20 val=GigabitEthernet0/4
    > AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
    > AVP: t=NAS-Port(5) l=6 val=50104
```

سمة مصدق الرسائل في طلب وصول Radius

فيما يلي مثال على التقاط طلب وصول لا يتضمن سمة مصدق الرسائل:

```
No.  | Time          | Source          | Destination     | Protocol | Length | Info
   1 | 11:33:57.435498 | 14.0.65.75      | 172.18.124.20   | RADIUS   |     99 | Access-Request id=12
   2 | 11:33:57.573576 | 172.18.124.20   | 14.0.65.75      | RADIUS   |     62 | Access-Reject id=12

> Frame 1: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
> Ethernet II, Src: Cisco_4a:81:02 (6c:b2:ae:4a:81:02), Dst: VMware_c9:84:88 (00:0c:29:c9:84:88)
> Internet Protocol Version 4, Src: 14.0.65.75, Dst: 172.18.124.20
> User Datagram Protocol, Src Port: 1645, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xc (12)
    Length: 57
    Authenticator: 82411d9bd5701fa8898885a0e69181a2
    [The response to this request is in frame 2]
  v Attribute Value Pairs
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=User-Name(1) l=7 val=jesse
    > AVP: t=Service-Type(6) l=6 val=Login(1)
    > AVP: t=NAS-IP-Address(4) l=6 val=14.0.65.75
```

التشفير باستخدام TLS/IPSec

أكثر الحلول فعالية على المدى البعيد لتأمين RADIUS هو تشفير حركة مرور البيانات بين خادم RADIUS و NAD. وهذا يضيف الكل من الخصوصية والسلامة التشفير الأقوى بمجرد الاعتماد على مصدق الرسائل المشتق من MD5-HMAC. والذي، إذا كان أي من هذه يمكن إستخدامه بين خادم RADIUS و NAD يعتمد على كل الجانبين اللذين يدعمان طريقة التشفير.

المصطلحات الواسعة المستخدمة عبر الصناعة لتشفير TLS ل RADIUS هي:

- "RadSec" - يشير إلى RFC 6614
- "RadSec TLS" - يشير إلى RFC 6614
- "DTLS ل RadSec" - يشير إلى RFC 7360

ومن المهم البدء في تنفيذ عملية الدمج طريقة خاضعة للرقابة نظرا لوجود مصروفات عامة للأداء في تشفير نظام النقل والإمداد فضلا عن اعتبارات إدارة الشهادات. كما سيتعين تجديد الشهادات بصورة منتظمة.

RADIUS عبر DTLS

يتم تحديد أمان طبقة نقل البيانات (DTLS) كطبقة نقل ل RADIUS بواسطة RFC 7360 الذي يستخدم الشهادات للمصادقة بشكل متبادل على خادم RADIUS ثم يوفر NAD بتشفير حزمة RADIUS بالكامل باستخدام نفق TLS. يبقى أسلوب النقل UDP ويتطلب نشر الشهادات على كل من خادم RADIUS و NAD. تذكر أنه عند نشر RADIUS عبر DTLS، من الضروري أن تتم إدارة انتهاء صلاحية الشهادة واستبدالها بشكل وثيق لمنع الشهادات منتهية الصلاحية من قطع اتصال RADIUS. يدعم ISE DTLS من أجل ISE إلى الاتصال، كما أن ISE 3.4 Radius over DTLS غير مدعوم لخوادم RADIUS-proxy أو RADIUS Token. كما يتم دعم RADIUS عبر DTLS بواسطة العديد من أجهزة Cisco التي تعمل كوقائع التحكم في الشبكة (NAD) مثل المحولات ووحدات التحكم اللاسلكية التي تعمل بنظام التشغيل IOS-XE®.

RADIUS عبر TLS

يتم تحديد تشفير أمان طبقة النقل (TLS) ل RADIUS بواسطة RFC 6614، ويغير النقل إلى TCP ويستخدم TLS لتشفير حزم RADIUS بالكامل. وتستخدم خدمة التعليمي هذا عادة كمثال. اعتبارا من ISE 3.4، ال يتم دعم RADIUS عبر TLS، ولكنه مدعوم من قبل العديد من (NADs) مثل المحولات ووحدات التحكم في الشبكة التي تعمل وقائع التحكم أجهزة Cisco التي تشغل IOS-XE.

IPsec

يتمتع محرك خدمات الهوية بدعم أصلي لأنفاق IPSec بين ISE و NADs التي تدعم أيضا إنهاء أنفاق IPSec. هذا خيار جيد حيث RADIUS عبر DTLS أو RADIUS عبر TLS غير مدعوم ولكن يجب إستخدامه بشكل محدود حيث يتم دعم 150 نفقا طقا لكل عقدة خدمات نهج ISE. لم يعد معيار ISE 3.3 والإصدارات اللاحقة يتطلب ترخيص IPSec، بل أصبح متوفرا الآن بطبيعته.

تخفيف جزئي

تجزئة RADIUS

حركة مرور المقطع RADIUS إلى شبكات VLAN الإدارية وارتباطات آمنة ومشفرة مثل ما يمكن توفيره عبر SD-WAN أو MACec. هذه الاستراتيجية لا تجعل خطر الهجوم صفرا، لكنها يمكن أن تقلل إلى حد كبير من سطح الهجوم في حالة الضعف. يمكن أن يكون ذلك مقياسا جيدا لتوقف الثغرات أثناء قيام المنتجات بطرح متطلبات مصدق الرسائل أو دعم DTLS/RadSec. ويتطلب الاستغلال أن يتواصل المهاجم بنجاح مع الدخيل (MITM) عبر نصف القطر بحيث لا يتمكن المهاجم من الوصول إلى مقطع الشبكة مع حركة المرور تلك، لا يمكن الهجوم. السبب في أن هذا تخفيف جزئي فقط هو أن تكوين الشبكة أو الحل الوسط لجزء من الشبكة يمكن أن يعرض حركة مرور RADIUS.

إذا تعذر تجزئة حركة مرور RADIUS أو تشفيرها، يمكن تنفيذ ميزات إضافية لمنع تشغيل MITM الناجح على الأجزاء المحفوفة بالمخاطر مثل: واقي مصدر بروتوكول الإنترنت (IP)، والفحص الديناميكي ل ARP، وتطفل بروتوكول التكوين الديناميكي للمضيف (DHCP). وقد يكون من الممكن أيضا إستخدام طرق مصادقة أخرى استنادا إلى نوع تدفق المصادقة مثل TACACS+ و SAML و LDAPs، وما إلى ذلك...

حالة الضعف لمحرك خدمات الهوية

الجداول التالية تصف المتوفر اعتبارا من ISE 3.4 لجعل تدفقات المصادقة محمية ضد شعاع الانفجار. للملخص، يجب وضع العناصر الثلاثة التالية في حالة تدفق باستخدام مصدق الرسائل فقط وليس تشفير DTLS/RadSec/IPSec، حتى لا يكون التدفق معرضا للخطر:
1) يجب أن يرسل جهاز الوصول إلى الشبكة سمة مصدق الرسائل في طلب الوصول.

2) يجب أن يتطلب خادم RADIUS سمة مصدق الرسائل في طلب الوصول.

3) يجب أن يستجيب خادم RADIUS بسمة مصدق الرسائل في تحدي الوصول وقبول الوصول ورفض الوصول.

يرجى الرجوع إلى CSCwk67747 الذي يتتبع التغييرات لإغلاق نقاط الضعف عندما يعمل ISE كعميل RADIUS.

ISE كخادم RADIUS

AAA Scenario	ISE Config	NAD capabilities	Status	Alternative options
EAP Protocols	--	--	Protected	
MAB, PAP, CHAP, MSCHAPv1/v2, Authorize-Only	Have on the checkbox "Require Message-Authenticator for all protocols"	Supports Message-Authenticator for non-EAP protocols	Protected	
		Doesn't support Message-Authenticator for non-EAP protocols	Vulnerable (because of NAD)	Can use IPsec
	Use RADIUS DTLS for this NAD	Supports RADIUS DTLS	Protected	
		Doesn't support RADIUS DTLS	Vulnerable (because of NAD)	Can use IPsec

ISE كعميل RADIUS

AAA Scenario	ISE Config	Peers' capabilities	Status	Alternative options
ISE as RADIUS Proxy	--	NAD supports Message-Authenticator **AND** RADIUS Server supports Message-Authenticator	Protected	
		NAD doesn't support Message-Authenticator **OR** RADIUS Server doesn't support Message-Authenticator	Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if both NAD and RADIUS Server use Message-Authenticator
ISE as RADIUS Token Client	--		Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if RADIUS Token Server uses Message-Authenticator
ISE as CoA Client	Configured to use Message-		Vulnerable (ISE must require	Can use IPsec Partial mitigation is achieved if Device Profiler checked option to use Message-Authenticator

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).