Blast-RADIUS(CVE-2024-3596)プロトコルスプーフィングの軽減

内容

はじめに

2024年7月7日、セキュリティ研究者はRADIUSプロトコルにおける次の脆弱性を公開しました。CVE-2024-3596:RFC 2865のRADIUSプロトコルは、MD5応答オーセンティケータシグニチャに対するchosen-prefix collision攻撃を使用して、他の応答への有効な応答（Access-Accept、Access-Reject、またはAccess-Challenge）を変更できるオンパス攻撃者によるが偽造攻撃のの影響をを受受受受受ける可能性可能性があります。同社は、https://www.blastradius.fail/pdf/radius.pdfで調査結果を詳しく説明した論文を公開しています。この論文は、Message-Authenticator属性を使用しないフローに対する応答偽造が成功したことを示しています。

この脆弱性の影響を受けるシスコ製品および修正を含むバージョンの最新リストについては、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3を参照してください。この記事では、一般的な緩和策と、すべてのシスコ製品ではなく一部の製品に対する緩和策の適用方法について説明します。具体的には、個々の製品ドキュメントを参照してください。シスコの主力RADIUSサーバであるIdentity Service Engineについては、さらに詳しく説明します。

背景

この攻撃は、MD5のコリジョンを利用する、MD5選択プレフィクス攻撃を利用します。これにより、攻撃者は、応答パケットの既存の属性を変更しながら、RADIUS応答パケットにデータを追加できます。実例として、RADIUS Access-RejectをRADIUS Access-Acceptに変更する機能を紹介しました。これが可能なのは、RADIUSではデフォルトでパケット内のすべての属性のハッシュが含まれていないためです。RFC 2869ではMessage-Authenticator（Mオーセンティケータ）属性が追加されていますが、現在のところ、この属性を含める必要があるのはEAPプロトコルを使用する場合だけです。つまり、RADIUSクライアント(NAD)にMessage-Authenticator（Mオーセンティケータ）属性が含まれていない非EAP交換に対しては、CVE-2024-3596で説明されている攻撃が可能です。

緩和

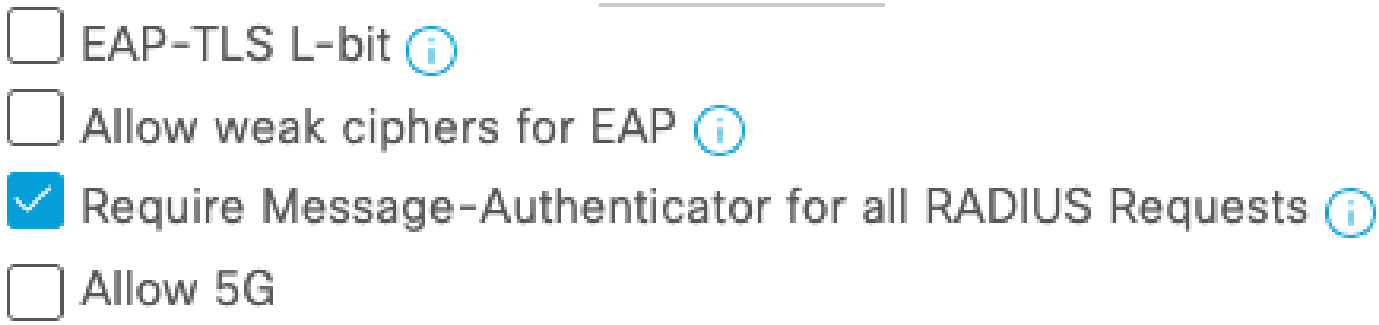
メッセージ認証者

1) RADIUSクライアントにはMessage-Authenticator属性が含まれている必要があります。

ネットワークアクセスデバイス(NAD)がAccess-RequestにMessage-Authenticator属性を含めると、Identity Services Engineは、結果としてすべてのバージョンのAccess-Accept、Access-Challenge、またはAccess-RejectパケットにMessage-Authenticatorを含めます。

2) RADIUSサーバは、Message-Authenticator属性の受信を強制する必要があります。

攻撃によって、RADIUSサーバに転送される前にアクセス要求からメッセージオーセンティケータを削除することが可能になるため、アクセス要求にメッセージオーセンティケータを含めるだけでは十分ではありません。RADIUSサーバでは、NADがアクセス要求にメッセージ認証者を含める必要もあります。これはIdentity Services Engineではデフォルトではありませんが、許可プロトコルレベルで有効にできます。これはポリシーセットレベルで適用されます。Allowed Protocols設定の下のオプションは、「Require Message-Authenticator for all RADIUS Requests」です。



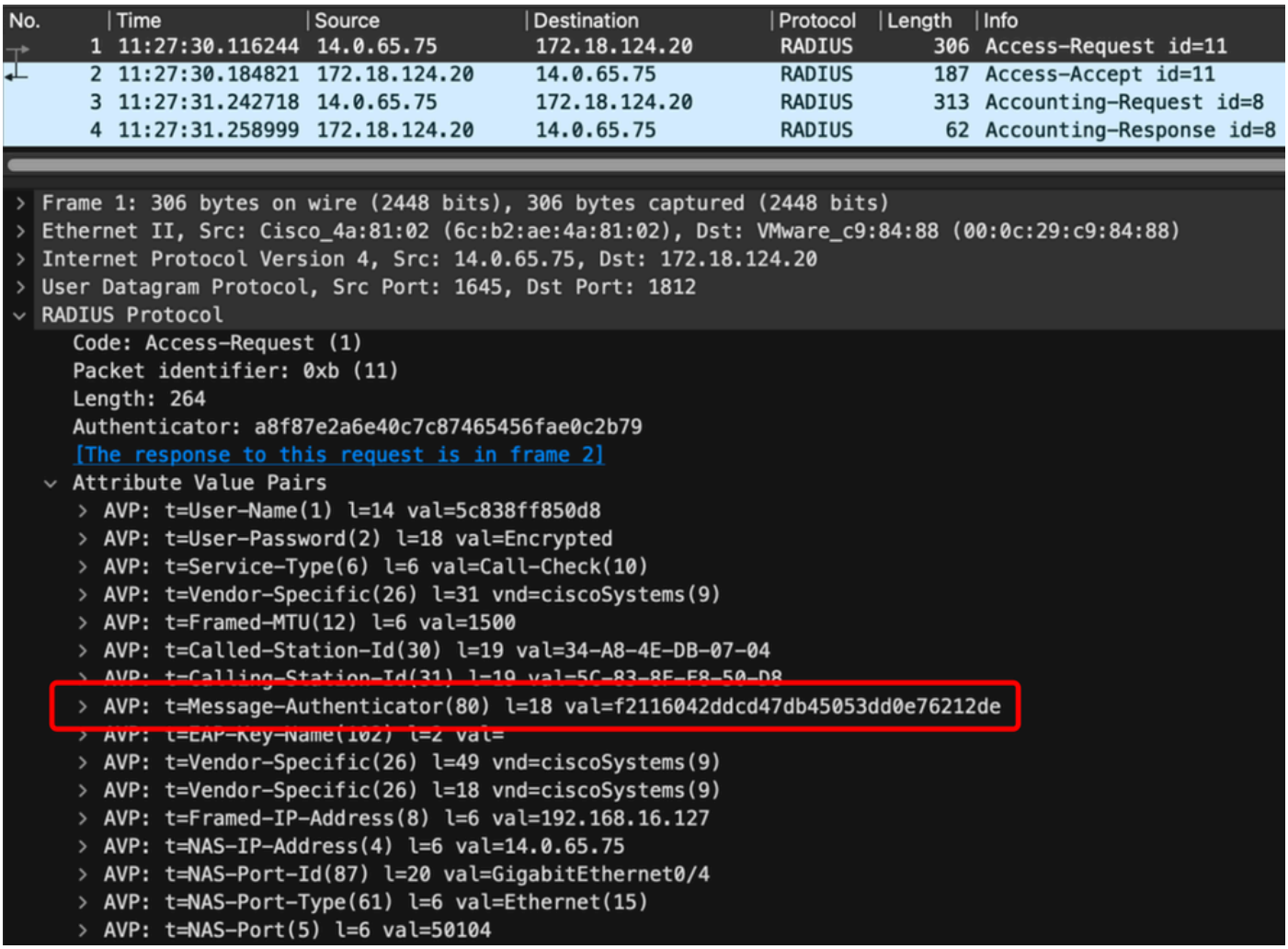
Identity Services EngineのAllowed Protocolsオプション

Allowed Protocols設定でMessage-Authenticatorが必要とされているが、Access-RequestにMessage-Authenticator属性が含まれていないポリシーセットと一致する認証は、ISEによってドロップされます。

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

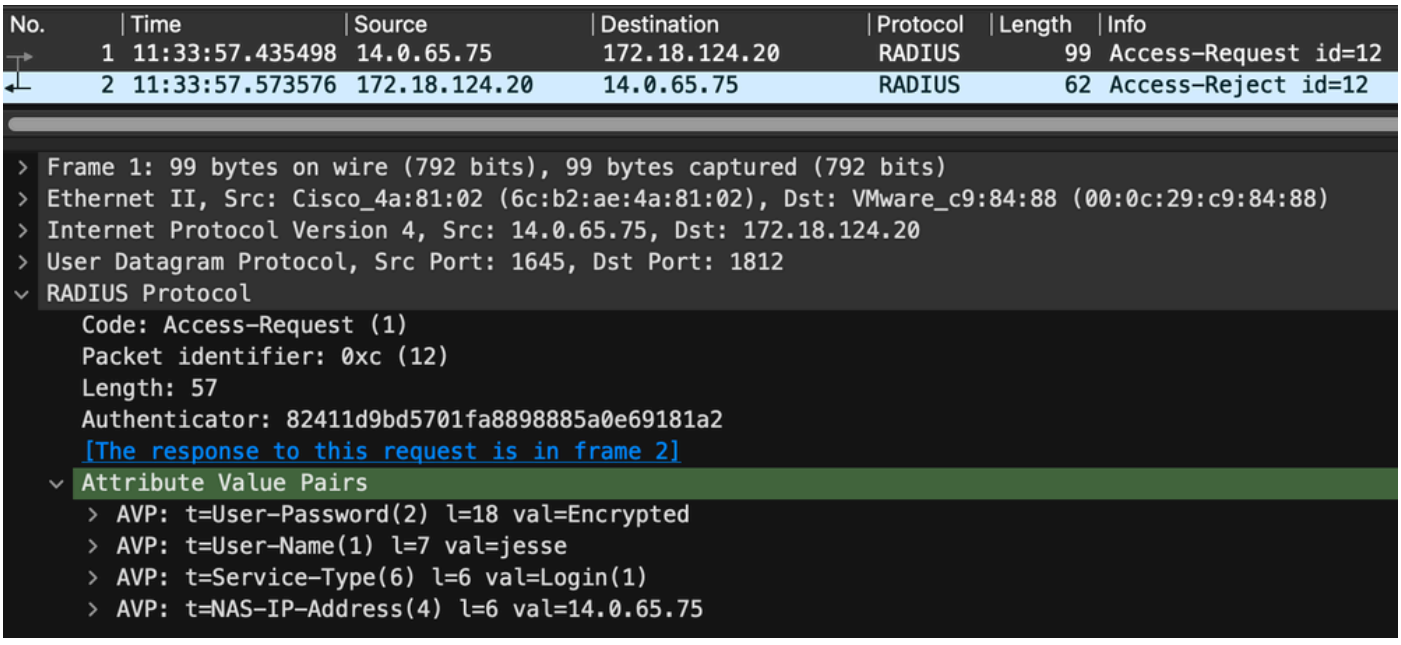
RADIUSサーバによって要求される前にNADがメッセージ認証子を送信しているかどうかを確認することが重要です。これはネゴシエートされる属性ではありません。メッセージ認証子を送信するのはNADの役割であり、デフォルトで送信するか、または送信するように設定されていることがNADの役割です。メッセージオーセンティケータは、ISEによって報告される属性の1つではありません。NADまたはユースケースにメッセージオーセンティケータが含まれているかどうかを判断するには、パケットキャプチャが最適な方法です。ISEには、「Operations」>「Troubleshoot」>「Diagnostic Tools」>「General Tools」>「TCP Dump」の順に選択したパケットキャプチャ機能が組み込まれています。同じNADの異なるユースケースには、メッセージ認証子を含めるかどうかも指定できることに注意してください。

Message-Authenticator属性を含むAccess-Requestのキャプチャ例を次に示します。



RADIUSアクセス要求のmessage-authenticator属性

次に、Message-Authenticator属性を含まないAccess-Requestのキャプチャ例を示します。



TLS/IPSecによる暗号化

RADIUSを保護するための最も効果的な長期的ソリューションは、RADIUSサーバとNAD間のトラフィックを暗号化することです。これにより、MD5-HMAC派生のメッセージ認証システムだけに依存するのではなく、プライバシーと強力な暗号化整合性の両方が追加されます。RADIUSサーバとNADの間でこれらのいずれかを使用できる場合は、暗号化方式をサポートする両側によって異なります。

RADIUSのTLS暗号化に業界で使用される幅広い用語は次のとおりです。

- 「RadSec」:RFC 6614を指します。
- 「RadSec TLS」:RFC 6614を指します。
- 「RadSec DTLS」:RFC 7360を指します。

TLS暗号化にはパフォーマンスのオーバーヘッドがあり、証明書管理の考慮事項もあるため、制御された方法で暗号化を展開することが重要です。証明書も定期的に更新する必要があります。

DTLS上のRADIUS

RADIUSのトランスポート層としてのDatagram Transport Layer Security(DTLS)はRFC 7360で定義されています。この定義では、証明書を使用してRADIUSサーバとNADが相互に認証し、TLSトンネルを使用して完全なRADIUSパケットを暗号化します。転送方式はUDPのままであり、証明書をRADIUSサーバとNADの両方に展開する必要があります。DTLS経由でRADIUSを導入する場合、期限切れの証明書によってRADIUS通信が中断されないように、証明書の期限切れと交換を綿密に管理する必要があります。ISEはISEからNADへの通信のDTLSをサポートしています。ISE 3.4では、RADIUS-ProxyまたはRADIUS Token ServerではRadius over DTLSはサポートされていません。RADIUS over DTLSは、IOS-XE®を実行するスイッチやワイヤレスコントローラなど、NADとして機能する多くのシスコデバイスでもサポートされています。

RADIUS over TLS（オプション）

RADIUSのTransport Layer Security(TLS)暗号化は、RFC 6614で定義されており、トランスポートをTCPに変更し、TLSを使用してRADIUSパケットを完全に暗号化します。これは、一般的にeduroamサービスで例として使用されます。ISE 3.4の時点では、RADIUS over TLSはサポートされていませんが、IOS-XEを実行するスイッチやワイヤレスコントローラなど、NADとして機能する多くのシスコデバイスでサポートされています。

IPSec

Identity Services Engine(ISE)は、ISEとNAD間のIPSecトンネルをネイティブでサポートし、IPSecトンネルの終了もサポートします。これは、RADIUS over DTLSまたはRADIUS over TLSがサポートされないような場合に適したオプションですが、ISEポリシーサービスノードあたり150トンネルしかサポートされないため、使用は控えてください。ISE 3.3以降ではIPSecのライセンスは不要になり、ネイティブで使用できるようになりました。

部分的な緩和

RADIUSセグメンテーション

RADIUSトラフィックを管理VLANにセグメント化し、SD-WANまたはMACSec経由で提供できるなどのセキュアで暗号化されたリンクを提供します。この戦略によって攻撃のリスクがゼロになることはありませんが、脆弱性の攻撃対象領域が大幅に縮小される可能性があります。これは、製品がメッセージオーセンティケータ要件またはDTLS/RadSecサポートを展開する際の適切な間隔の測定になります。この不正利用には、攻撃者がRADIUS通信の中間者(MITM)を特定する必要があります。そのため、攻撃者がそのトラフィックを含むネットワークセグメントにアクセスできない場合、攻撃を受ける可能性はありません。これが部分的な緩和策にすぎない理由は、ネットワークの設定ミスやネットワークの一部の侵害によって、RADIUSトラフィックが露出する可能性があるためです。

RADIUSトラフィックをセグメント化または暗号化できない場合は、IPソースガード、ダイナミックARPインスペクション、DHCPスヌーピングなどの追加の機能を実装して、リスクのあるセグメントでのMITMの成功を防ぐことができます。TACACS+、SAML、LDAPSなど、認証フローのタイプに基づいて他の認証方式を使用することもできます。

Identity Services Engineの脆弱性ステータス

次の表では、Blast-RADIUSから認証フローを保護するためにISE 3.4で使用可能な機能について説明します。要約すると、フローが脆弱にならないように、次の3つの項目がメッセージ認証機能のみを使用するフローに対して適切であり、DTLS/RadSec/IPSec暗号化を使用していない必要があります。
1)ネットワークアクセスデバイスは、Access-RequestでMessage-Authenticator属性を送信する必要があります。

2) RADIUSサーバは、Access-RequestでMessage-Authenticator属性を必要とします。

3) RADIUSサーバは、Access-Challenge、Access-Accept、およびAccess-RejectのMessage-Authenticator属性で応答する必要があります。

ISEがRADIUSクライアントとして動作しているときに脆弱性を閉じるための変更を追跡している[CSCwk67747]を参照してください。

RADIUSサーバとしてのISE

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

RADIUSクライアントとしてのISE

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。