Blast-RADIUS (CVE-2024-3596)協定偽裝緩解

目錄

簡介

2024年7月7日，安全研究人員在RADIUS協定中披露了以下漏洞：CVE-2024-3596：RFC 2865下的RADIUS協定容易受到路徑上攻擊者的偽造攻擊，該攻擊者可以利用針對MD5響應身份驗證器簽名選擇的字首衝突攻擊修改任何有效的響應（Access-Accept、Access-Reject或Access-Challenge）到任何其他響應。他們在https://www.blastradius.fail/pdf/radius.pdf上發表了一篇文章，詳細介紹了其發現。這篇文章對未使用Message-Authenticator屬性的流進行了成功的響應偽造。

有關受此漏洞影響的思科產品的最新清單以及包含修復的版本，請訪問：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3。本文將介紹一般緩解技術以及它們如何應用於某些（但不是全部）思科產品，具體資訊請參閱單個產品文檔。身為Cisco的旗艦級RADIUS伺服器，身份服務引擎將詳細介紹。

背景

此攻擊利用MD5中的衝突進行MD5選擇字首攻擊，使得攻擊者能夠在修改響應資料包的現有屬性的同時，向RADIUS響應資料包增加附加資料。一個示例展示了將RADIUS Access-Reject更改為RADIUS Access-Accept的能力。可行的原因是RADIUS預設不包含封包中所有屬性的雜湊。RFC 2869確實增加了消息驗證器屬性，但是當前僅當使用EAP協定時才需要包括它，這意味著對於任何RADIUS客戶端(NAD)不包含消息驗證器屬性的非EAP交換，都可能發生CVE-2024-3596中描述的攻擊。

緩解

消息驗證器

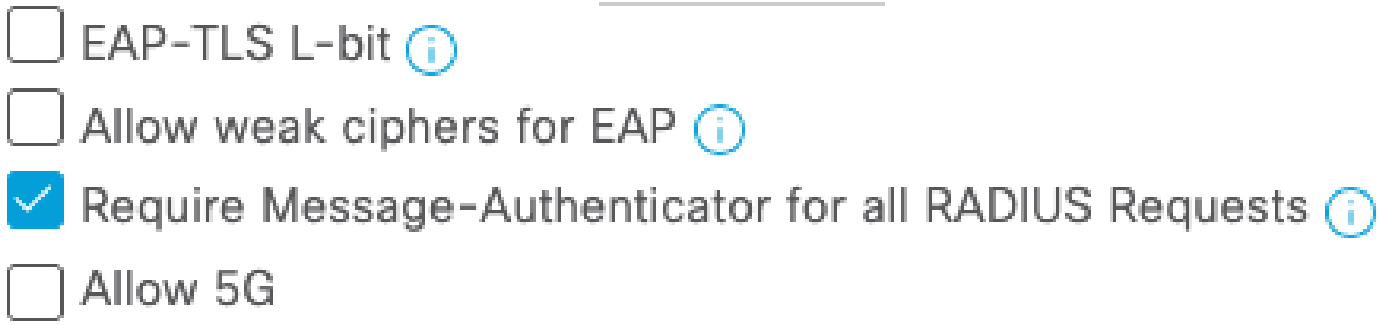
1) RADIUS客戶端必須包括Message-Authenticator屬性。

當網路接入裝置(NAD)在Access-Request中包含Message-Authenticator屬性時，身份服務引擎將在所有版本中產生的Access-Accept、Access-Challenge或Access-Reject資料包中包含Message-Authenticator。

2) RADIUS伺服器必須強制接收Message-Authenticator屬性。

僅僅在訪問請求中包含消息身份驗證器是不夠的，因為攻擊使得可以在將消息身份驗證器轉發到RADIUS伺服器之前從訪問請求中刪除該消息身份驗證器。RADIUS伺服器還必須要求NAD在Access-Request中包含消息身份驗證器。這不是身份服務引擎的預設設定，但可以在允許的協定級別（在策略集級別應用）啟用。「Allowed Protocols」配置下的選項為「Require Message-

Authenticator」（對於所有RADIUS請求）：



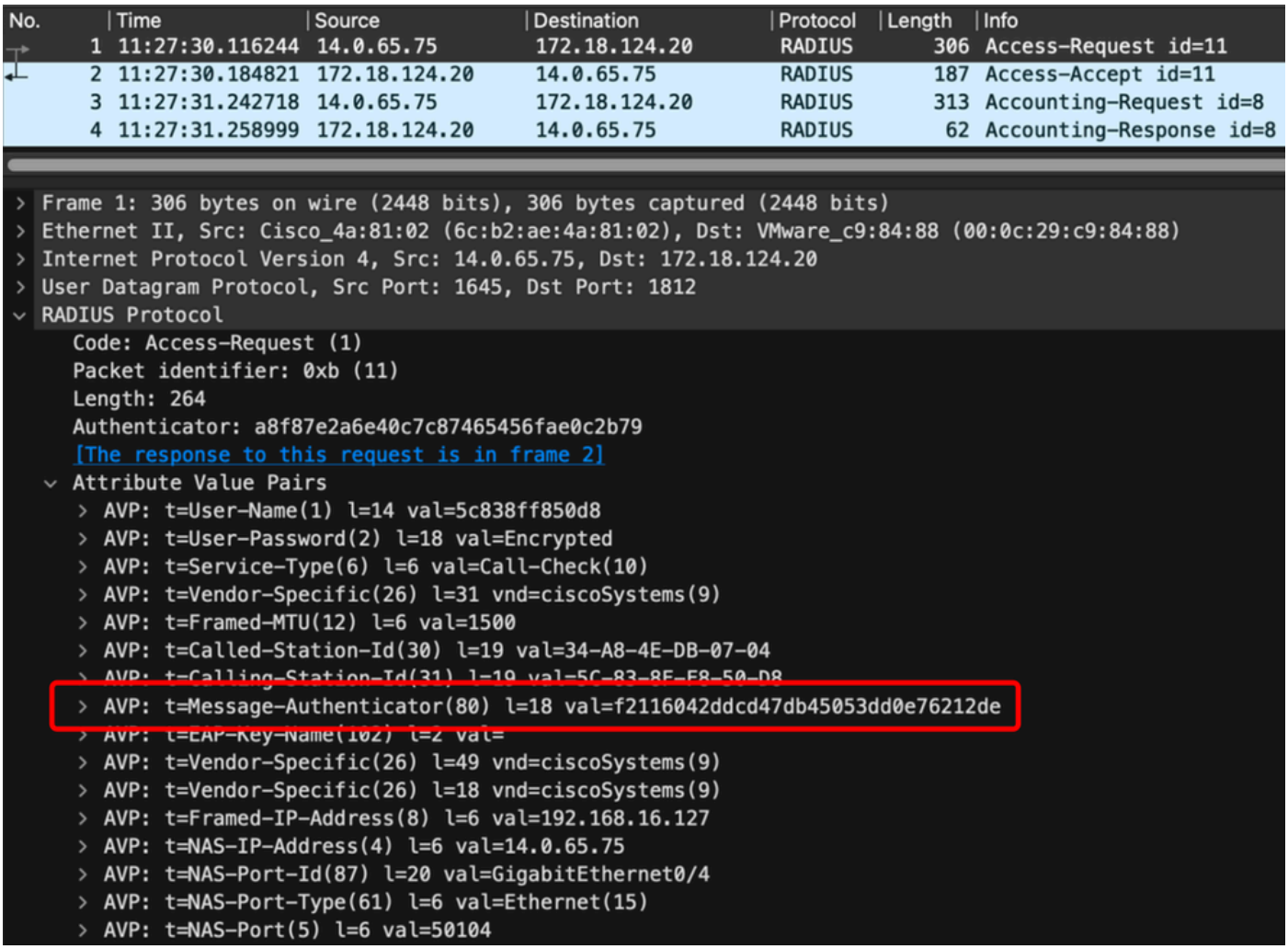
身份服務引擎中的「允許的協定」選項

與Allowed Protocols配置需要Message-Authenticator但Access-Request不包含Message-Authenticator屬性的策略集匹配的身份驗證將被ISE丟棄：

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

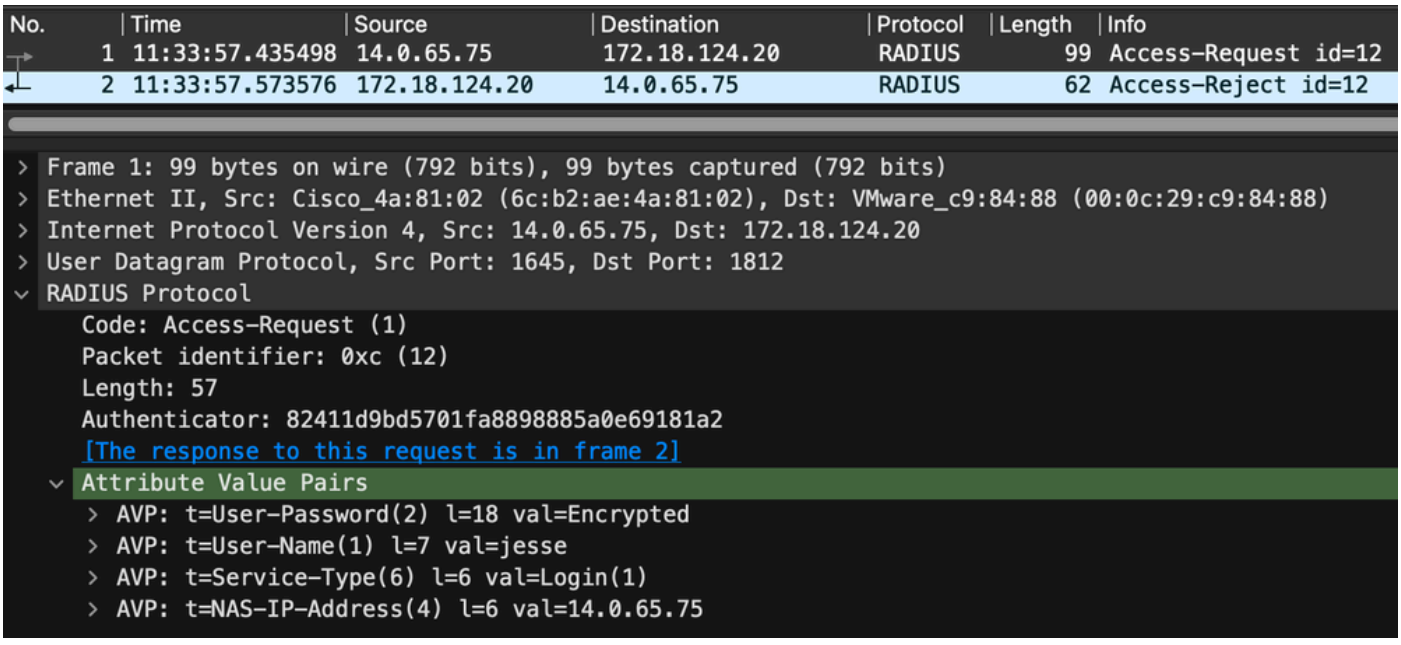
在要求RADIUS伺服器傳送消息驗證程式之前，必須驗證NAD是否正在傳送消息驗證程式，因為這不是協商的屬性，NAD在預設情況下傳送消息驗證程式或將其配置為傳送消息驗證程式。消息驗證器不是ISE報告的屬性之一，資料包捕獲是確定NAD/使用案例是否包括消息驗證器的最佳方法。ISE在Operations -> Troubleshoot -> Diagnostic Tools -> General Tools -> TCP Dump下內建資料包捕獲功能。請記住，來自同一NAD的不同用例可以包含或不包含消息驗證器。

以下是包含Message-Authenticator屬性的Access-Request的示例捕獲：



Radius access-request中的Message-authenticator屬性

以下是不包含Message-Authenticator屬性的訪問請求的示例捕獲：



使用TLS/IPSec加密

保護RADIUS的最有效長期解決方案是加密RADIUS伺服器與NAD之間的流量。這增加了隱私性和更強的加密完整性，而不僅僅是依賴MD5-HMAC派生的消息驗證器。如果RADIUS伺服器和NAD之間可以使用其中任何一種，則取決於支援加密方法的雙側。

業界對RADIUS的TLS加密所使用的術語包括：

- 「RadSec」-指RFC 6614
- 「RadSec TLS」-指RFC 6614
- 「RadSec DTLS」-指RFC 7360

由於存在TLS加密的效能開銷以及證書管理注意事項，因此以可控的方式推廣加密非常重要。證書也必須定期更新。

使用DTLS的RADIUS

RFC 7360將資料包傳輸層安全(DTLS)定義為RADIUS的傳輸層，它使用證書對RADIUS伺服器進行相互身份驗證，然後使用TLS隧道加密完整的RADIUS資料包。傳輸方法仍為UDP，並且需要在RADIUS伺服器和NAD上部署證書。請記住，在透過DTLS部署RADIUS時，必須嚴格管理證書到期和替換，以防止過期的證書中斷RADIUS通訊。ISE支援DTLS進行ISE到需要通訊，自ISE 3.4 Radius over DTLS不受RADIUS-Proxy或RADIUS令牌伺服器支援。許多思科裝置(例如運行IOS-XE®的交換機和無線控制器)也支援DTLS上的RADIUS。

使用TLS的RADIUS

RADIUS的傳輸層安全(TLS)加密由RFC 6614定義，將傳輸更改為TCP並使用TLS對RADIUS資料包進行完全加密。通常以eduroam服務為例。自ISE 3.4起，不支援基於TLS的RADIUS，但許多充當需要的NAD的思科裝置（例如運行IOS-XE的交換機和無線控制器）都支援此功能。

IPSec

身份服務引擎對ISE和NAD之間的IPSec隧道提供本地支援，同時支援終端IPSec隧道。這是不支援RADIUS over DTLS或RADIUS over TLS的良好選項，但應謹慎使用，因為每個ISE原則服務節點只支援150個通道。ISE 3.3及更高版本不再需要IPSec許可證，現在可本地使用。

部分緩解

RADIUS分段

將RADIUS流量分段到管理VLAN和安全的加密鏈路，例如可以透過SD-WAN或MACSec提供。此策略不會將攻擊風險降至零，但可以大大減少漏洞的攻擊面。當產品推出消息驗證器要求或DTLS/RadSec支援時，這可以是一個很好的間隔措施。此漏洞需要攻擊者成功透過RADIUS通訊進行中間人(MITM)，因此，如果攻擊者無法使用該流量進入網段，則不可能發起攻擊。這僅是部分緩解措施的原因在於，網路配置錯誤或網路的一部分受到危害可能暴露RADIUS流量。

如果無法對RADIUS流量進行分段或加密，則可以實施其他功能來阻止風險段上成功的MITM，例如：IP源防護、動態ARP檢測和DHCP監聽。還可以利用基於認證流型別的其它認證方法，例如

TACACS+、SAML、LDAPS等。

身份服務引擎漏洞狀態

下表介紹從ISE 3.4起，使身份驗證流受到防禦Blast-RADIUS的可用功能。要重述，對於僅使用消息驗證器而不使用DTLS/RadSec/IPSec加密的流，以下三個專案必須處於就緒狀態，這樣該流才能不易受攻擊：
1)網路接入裝置必須傳送Access-Request中的Message-Authenticator屬性。

2) RADIUS伺服器必須在Access-Request中要求Message-Authenticator屬性。

3) RADIUS伺服器必須在Access-Challenge、Access-Accept和Access-Reject中以Message-Authenticator屬性做出響應。

當ISE充當RADIUS客戶端時，請參閱CSCwk67747，它正在跟蹤更改以關閉漏洞。

ISE作為RADIUS伺服器

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

作為RADIUS客戶端的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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。