Blast-RADIUS (CVE-2024-3596)协议伪装缓解

目录

简介

2024年7月7日，安全研究人员披露了RADIUS协议中的以下漏洞：CVE-2024-3596：RFC 2865下的RADIUS协议易受路径上攻击者的伪造攻击，攻击者可以使用针对MD5响应身份验证器签名的选择前缀冲突攻击将任何有效的响应（Access-Accept、Access-Reject或Access-Challenge）修改为任何其他响应。他们在https://www.blastradius.fail/pdf/radius.pdf上发布了一篇论文，其中详细说明了他们的发现。该论文证明，在不使用“消息身份验证器”属性的流中发生了成功的响应伪造。

有关受此漏洞影响的思科产品的最新列表以及包含修复程序的版本，请访问：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3。本文将介绍一般缓解技术以及它们如何适用于某些（但不是所有）思科产品，具体内容应参阅个别产品文档。作为思科的旗舰RADIUS服务器，身份服务引擎将会详细介绍。

背景

此攻击利用MD5中利用冲突的MD5选择前缀攻击，使攻击者能够在修改响应数据包的现有属性的同时向RADIUS响应数据包添加其他数据。演示的一个示例是将RADIUS Access-Reject更改为RADIUS Access-Accept的能力。这是可能的，因为RADIUS默认情况下不包含数据包中所有属性的散列。RFC 2869确实添加了“消息-身份验证器”属性，但当前仅要求使用EAP协议时包含它，这意味着对RADIUS客户端(NAD)不包含“消息-身份验证器”属性的任何非EAP交换，都可能出现CVE-2024-3596中描述的攻击。

缓解

消息验证器

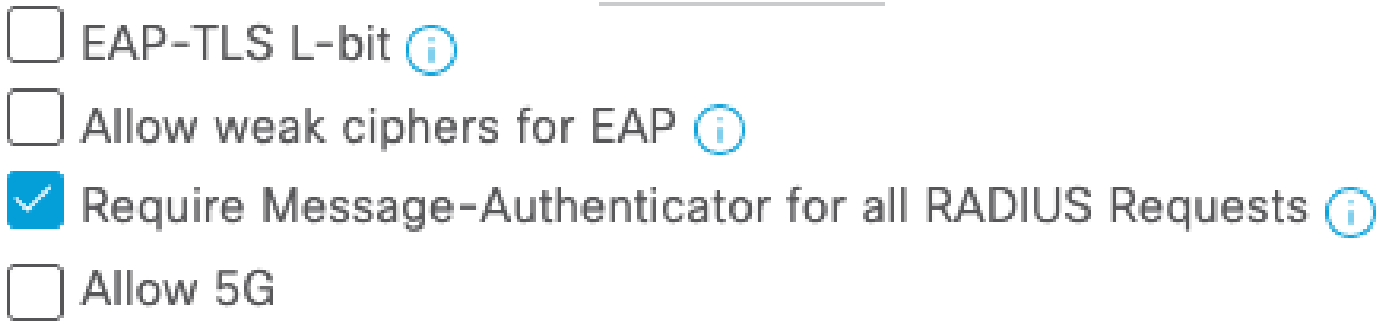
1) RADIUS客户端必须包含消息验证器属性。

当网络接入设备(NAD)在Access-Request中包含Message-Authenticator属性时，身份服务引擎将在所有版本中生成的Access-Accept、Access-Challenge或Access-Reject数据包中包含Message-Authenticator。

2) RADIUS服务器必须强制接收Message-Authenticator属性。

仅仅在访问请求中包含消息身份验证器是不够的，因为攻击可以在将消息身份验证器转发到RADIUS服务器之前从访问请求中删除该消息身份验证器。RADIUS服务器还必须要求NAD在Access-Request中包含消息身份验证器。这不是身份服务引擎的默认设置，但可以在允许的协议级别（在策略集级别应用）启用。Allowed Protocols配置下的选项是“Require Message-

Authenticator” for all RADIUS Requests”：



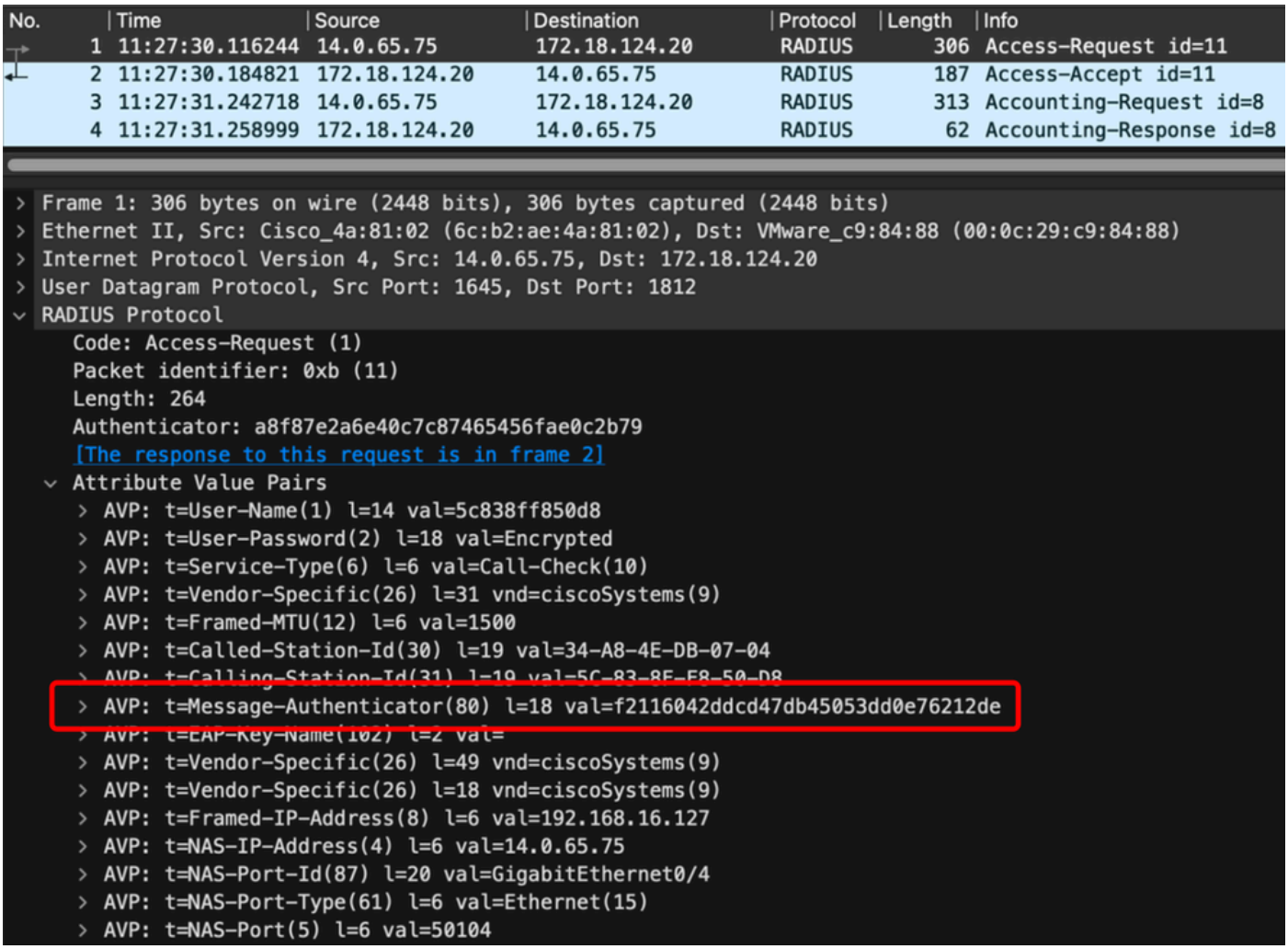
身份服务引擎中的“允许的协议”选项

与策略集匹配的身份验证，其中Allowed Protocols配置需要Message-Authenticator，但Access-Request不包含Message-Authenticator属性时，ISE将丢弃以下身份验证：

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

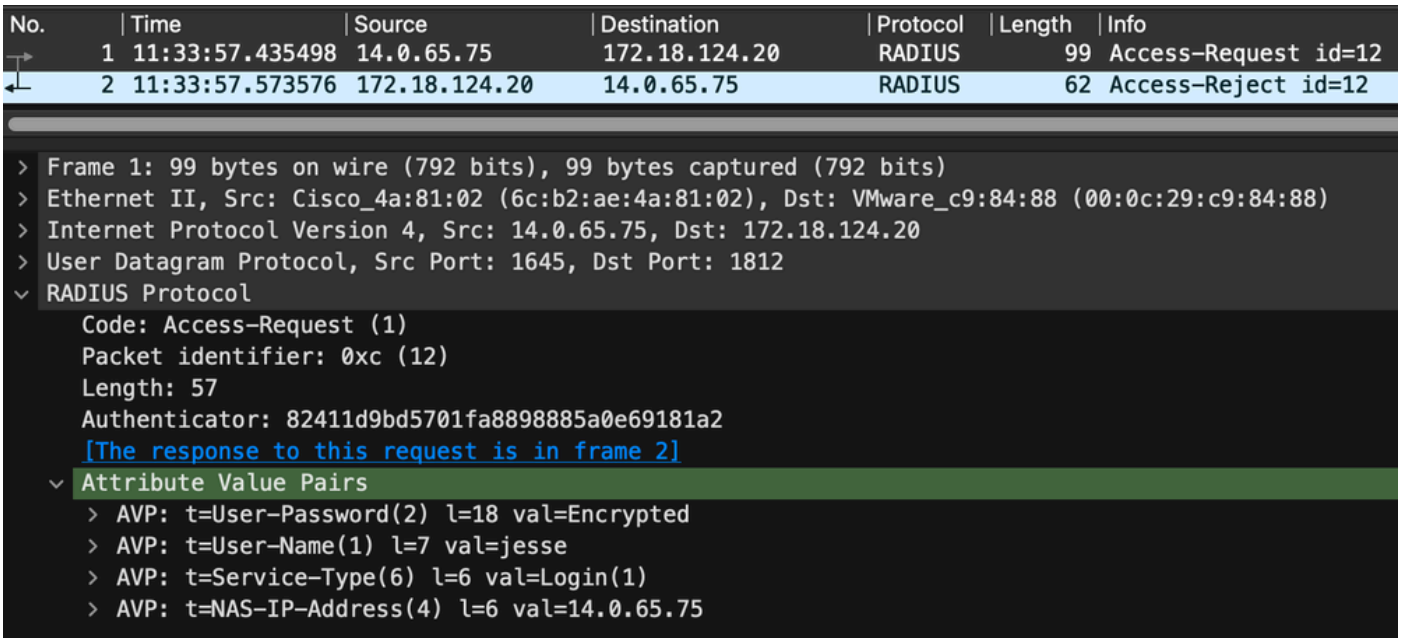
在需要由RADIUS服务器之前验证是否需要发送消息验证器非常重要，因为这不是协商的属性，NAD负责在默认情况下发送消息验证器或将其配置为发送消息。消息身份验证器不是ISE报告的属性之一，数据包捕获是确定NAD/使用案例是否包含消息身份验证器的最佳方法。ISE在Operations -> Troubleshoot -> Diagnostic Tools -> General Tools -> TCP Dump下内置了数据包捕获功能。请记住，来自同一NAD的不同使用案例可以包括或不包括消息身份验证器。

以下是包含Message-Authenticator属性的Access-Request的示例捕获：



Radius access-request中的消息身份验证器属性

以下是不包含消息身份验证器属性的访问请求的捕获示例：



使用TLS/IPSec加密

保护RADIUS的最有效的长期解决方案是加密RADIUS服务器和NAD之间的流量。与仅依赖MD5-HMAC派生的消息验证器相比，这增加了隐私性和更强的加密完整性。如果RADIUS服务器和NAD之间可以使用其中任何一种，则取决于两端是否支持加密方法。

业内对RADIUS的TLS加密使用的广泛术语包括：

- “RadSec”-指RFC 6614
- “RadSec TLS”-指RFC 6614
- “RadSec DTLS”-指RFC 7360

由于存在TLS加密的性能开销以及证书管理注意事项，因此以受控方式推广加密非常重要。证书也必须定期更新。

基于DTLS的RADIUS

RFC 7360将数据报传输层安全(DTLS)定义为RADIUS的传输层。此协议使用证书对RADIUS服务器进行相互身份验证，然后需要使用TLS隧道加密完整的RADIUS数据包。传输方法仍为UDP，并且需要在RADIUS服务器和NAD上部署证书。请记住，在通过DTLS部署RADIUS时，必须严格管理证书到期和替换，以防止过期的证书中断RADIUS通信。ISE支持ISE到需要通信的DTLS，因为RADIUS代理或RADIUS令牌服务器不支持ISE 3.4 Radius over DTLS。许多思科设备也支持DTLS上的RADIUS，这些设备充当NAD，例如运行IOS-XE®的交换机和无线控制器。

基于TLS的RADIUS

RFC 6614中定义了RADIUS的传输层安全(TLS)加密，将传输更改为TCP并使用TLS完全加密RADIUS数据包。通常以eduroam服务为例。自ISE 3.4起，不支持基于TLS的RADIUS，但许多作为NAD的思科设备都支持RADIUS，例如运行IOS-XE的交换机和无线控制器。

IPsec

身份服务引擎对ISE和NAD之间的IPSec隧道提供本地支持，也支持终端IPSec隧道。这是不支持RADIUS over DTLS或RADIUS over TLS的一个好选项，但应谨慎使用，因为每个ISE策略服务节点仅支持150个隧道。ISE 3.3及更高版本不再需要用于IPSec的许可证，现在可在本地使用。

部分缓解

RADIUS分段

将RADIUS流量分段到管理VLAN和安全的加密链路，例如可以通过SD-WAN或MACSec提供。这种策略不会使攻击风险降至零，但可以大大减小漏洞的攻击面。当产品推出消息验证器要求或DTLS/RadSec支持时，这可以作为一种很好的停止间隙措施。此漏洞要求攻击者成功实现RADIUS通信的中间人(MITM)，因此，如果攻击者无法通过该流量进入网段，将无法发起攻击。这仅是部分缓解的原因是，网络配置错误或网络部分受损可能会暴露RADIUS流量。

如果RADIUS流量无法分段，或者可以实施其他功能来阻止有风险分段上的MITM成功，例如：IP源防护、动态ARP检测和DHCP监听。还可以根据身份验证流类型使用其他身份验证方法，例如

TACACS+、SAML、LDAPS等。

身份服务引擎漏洞状态

下表介绍自ISE 3.4起，可用于使身份验证流针对Blast-RADIUS提供保护的内容。要概括，对于仅使用消息验证器而不使用DTLS/RadSec/IPSec加密的流，必须满足以下3项要求，才能使流不易受攻击：
1)网络接入设备必须发送Access-Request中的Message-Authenticator属性。

2) RADIUS服务器必须在Access-Request中要求Message-Authenticator属性。

3) RADIUS服务器必须在Access-Challenge、Access-Accept和Access-Reject中使用Message-Authenticator属性进行响应。

当ISE用作RADIUS客户端时，请参阅CSCwk67747跟踪更改以关闭漏洞的章节。

ISE作为RADIUS服务器

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

ISE作为RADIUS客户端

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。