Blast-RADIUS (CVE-2024-3596) Protocol Spoofing Mitigation

Contents

Introduction

On July 7, 2024, security researchers disclosed the following vulnerability in the RADIUS protocol: CVE-2024-3596: RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. They have published a paper detailing their findings at <u>https://www.blastradius.fail/pdf/radius.pdf</u> which demonstrates a successful response forgery against flows that do not utilize the Message-Authenticator attribute.

For an up to date list of Cisco products impacted by this vulnerability and versions that contain fixes please visit: <u>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3</u>. This article will cover general mitigation techniques as well as how they apply to some, but not all Cisco products, individual product documentation should be consulted for specifics. As Cisco's flagship RADIUS server, Identity Service Engine will be covered in more detail.

Background

This attack takes advantage of an MD5 chosen-prefix attack utilizing collisions in MD5, which allows an attacker to add additional data to the RADIUS response packet while modifying existing attributes of the response packet. An example demonstrated was the ability to change a RADIUS Access-Reject into a RADIUS Access-Accept. This is possible because RADIUS by default does not include a hash of all attributes in the packet. <u>RFC 2869</u> does add the Message-Authenticator attribute but it is currently only required to be included when using EAP protocols, meaning the attack describe in CVE-2024-3596 is possible against any non-EAP exchange where the RADIUS Client (NAD) does not include the Message-Authenticator attribute.

Mitigation

Message-Authenticator

1) RADIUS client must include Message-Authenticator attribute.

When the Network Access Device (NAD) includes the Message-Authenticator attribute in the Access-Request, Identity Services Engine will include Message-Authenticator in the resulting Access-Accept, Access-Challenge, or Access-Reject packet in all versions.

2) The RADIUS server must enforce receiving the Message-Authenticator attribute.

It isn't enough to just include the Message-Authenticator in the Access-Request as the attack makes it possible to strip the Message-Authenticator from the Access-Request before it is forwarded to the RADIUS Server. The RADIUS Server must also require the NAD to include Message-Authenticator in the Access-Request. This is not default on Identity Services Engine but can be enabled at the allowed protocols level,

which applies at the policy set level. The option under the Allowed Protocols configuration is "Require Message-Authenticator" for all RADIUS Requests":



Authentications that match a policy set where the Allowed Protocols configuration requires Message-Authenticator, but where the Access-Request does not contain the Message-Authenticator attribute will be dropped by ISE:

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

It is important to verify whether the NAD is sending Message-Authenticator before being require by the RADIUS Server as this is not a negotiated attribute, it is up to the NAD to send it either by default or be configured to send it. Message-Authenticator is not one of the attributes reported by ISE, a packet capture is the best way to determine if a NAD/Use Case is including Message-Authenticator. ISE has built in packet capture functionality under Operations -> Troubleshoot -> Diagnostic Tools -> General Tools -> TCP Dump. Keep in mind that different use cases from the same NAD can either include or not include Message-Authenticator.

The following is an exmple capture of an Access-Request that includes the Message-Authenticator attribute:

No.	. Tim	9	Source	Destination	Protocol	Length Info	
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	1 11:	27:30.116244	14.0.65.75	172.18.124.20	RADIUS	306 Acc	cess-Request id=11
₄⊥	2 11:	27:30.184821	1/2.18.124.20	14.0.05.75	RADIUS	187 ACC	cess-Accept 1d=11
	3 11:	27:31.242/18	14.0.05./5	1/2.18.124.20	RADIUS	513 ACC	counting_Request 1d=8
	4 11:	27:31.258999	172.18.124.20	14.0.05.75	RADIUS	62 ACC	counting-Response 1d=8
-	_						
>	Frame 1:	306 bytes on	wire (2448 bit	s), 306 bytes captured	(2448 bit	s)	
>	Ethernet	II, Src: Cis	co_4a:81:02 (6c	:b2:ae:4a:81:02), Dst:	VMware_c9	:84:88 (00:00	c:29:c9:84:88)
>	Internet	Protocol Ver	sion 4, Src: 14	.0.65.75, Dst: 172.18.	124.20		
>	User Data	gram Protoco	l, Src Port: 16	45, Dst Port: 1812			
\sim	RADIUS Pr	otocol					
	Code: /	ccess-Reques	t (1)				
	Packet	identifier:	0xb (11)				
	Length	264					
	Authen	icator: a8f8	7e2a6e40c7c8746	55456fae0c2b79			
	[The re	sponse to th	is request is i	<u>in frame 2]</u>			
	✓ Attrib	ite Value Pai	.rs				
	> AVP:	t=User-Name	(1) l=14 val=5c	838ff850d8			
	> AVP: t=User-Password(2) l=18 val=Encrypted						
	> AVP: t=Service-Type(6) l=6 val=Call-Check(10)						
	<pre>> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)</pre>						
	<pre>> AVP: t=Framed-MTU(12) l=6 val=1500</pre>						
	> AVP:	t=Called-St	ation-Id(30) l=	19 val=34-A8-4E-DB-07-	-04		
	AVP: t=Calling=Station=Td(31) 1=10 val=5C=83=8E=E8=50=08						
	> AVP:	t=Message-A	uthenticator(80) l=18 val=T2116042ddc -	:d4/db45053	dd0e/6212de	
	> AVP:		ame(102) l=2 va				
	> AVP;	t=Vendor-Sp	ecli1c(26) l=49	vnd=ciscoSystems(9)			
	> AVP:	t=venuor-sp	$\frac{1}{2}$	vnu=ciscosystems(9)			
	> AVP:		-Audress(0) (=0				
	> AVP;	t=NAS-IP-Au	uress(4) (=0 va td(97) 1-20 val	-CiabitEthernot(//			
	> AVP;	t-NAS-PORT-	$T_{VDP}(61) = 20 Val$	-organicethernet(15)			
	> AVP;	t-NAS-PORt-	5) 1-6 val-5010				
	> AVP: > AVP: > AVP: > AVP: > AVP:	t=NAS-IP-Ad t=NAS-Port- t=NAS-Port- t=NAS-Port(dress(4) l=6 va Id(87) l=20 val Type(61) l=6 va 5) l=6 val=5010	l=14.0.65.75 =GigabitEthernet0/4 l=Ethernet(15) 4			

Message-authenticator attribute in Radius access-request

The following is an example capture of an Access-Request that does not include the Message-Authenticator attribute:

No. ⊤*	. Time 1 11:33:57.435498	Source	Destination 172.18.124.20	Protocol Le RADIUS	ength Info 99 Access-Request i	id=12	
₄∟	2 11:33:57.573576	172.18.124.20	14.0.65.75	RADIUS	62 Access-Reject id	d=12	
						_	
> >	Frame 1: 99 bytes on w Ethernet II, Src: Cisc	vire (792 bits), co_4a:81:02 (6c:1	99 bytes captured b2:ae:4a:81:02), Ds	(792 bits) t: VMware_c9:84:	:88 (00:0c:29:c9:84:88))	
ζ.	Internet Protocol vers	STON 4, STC: 14.0	0.03.73, USL: 172.1 5	0.124.20			
ý	RADIUS Protocol	, 510 1010, 104.	5, 531 1012				
	Code: Access-Reques Packet identifier: Length: 57 Authenticator: 8241	t (1) 0xc (12) 1d9bd5701fa88988	85a0e69181a2				
	[Ine response to this request is in trame 2]						
	<pre>> AVP: t=User-Pass > AVP: t=User-Name > AVP: t=Service-Ty > AVP: t=NAS-IP-Ade</pre>	vord(2) l=18 val: (1) l=7 val=jess vpe(6) l=6 val=L dress(4) l=6 val:	=Encrypted e ogin(1) =14.0.65.75				

Encrypt with TLS/IPSec

The most effective long term solution to secure RADIUS is to encrypt the traffic between the RADIUS Server and the NAD. This adds both privacy and stronger cryptographic integrity over just relying on the MD5-HMAC derived Message-Authenticator. Which, if any of these can be used between the RADIUS Server and the NAD depend on both sides supporting the encryption method.

The broad terms used across the industry for TLS Encryption of RADIUS are:

- "RadSec" refers to RFC 6614
- "RadSec TLS" refers to RFC 6614
- "RadSec DTLS" refers to RFC 7360

It is important to roll out encrytion in a controlled manner as there is performance overhead to TLS encryption as well as certificate management considerations. Certificates will also have to be renewed on a regular basis.

RADIUS over DTLS

Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS is defined by <u>RFC 7360</u> which uses certificates to mutually authenticate the RADIUS Server and the NAD then encrypts the full RADIUS packet using a TLS tunnel. The transport method remains UDP and requires certificates to be deployed on both the RADIUS Server and NAD. Keep in mind that when deploying RADIUS over DTLS, it is imperative that certificate expiry and replacement is closely managed to prevent expired certificates from interrupting RADIUS communication. ISE supports DTLS for ISE to NAD communication, as of ISE 3.4 Radius over DTLS is not supported for RADIUS-Proxy or RADIUS Token Servers. RADIUS over DTLS is also supported by many Cisco devices that act as NADs such as switches and wireless controllers running IOS-XE®.

RADIUS over TLS

Transport Layer Security (TLS) Encryption for RADIUS is defined by <u>RFC 6614</u>, changes the transport to TCP and uses TLS to fully encrypt RADIUS packets. This is commonly used by the eduroam service as an example. As of ISE 3.4, RADIUS over TLS is not supported, but is supported by many Cisco devices that act as NADs such as switches and wireless controllers running IOS-XE.

IPSec

Identity Services Engine has native support for IPSec tunnels between ISE and NADs that also support terminating IPSec tunnels. This is a good option where RADIUS over DTLS or RADIUS over TLS is not supported but should be used sparingly as only 150 tunnels are supported per ISE Policy Services Node. ISE 3.3 and later no longer requires a license for IPSec, it is now available natively.

Partial Mitigation

RADIUS Segmentation

Segment RADIUS traffic to management VLANs and secure, encrypted links such as can be provided via SD-WAN or MACSec. This strategy does not bring the risk of the attack to zero but can greatly reduce the attack surface of the vulnerability. This can be a good stop gap measure while products roll out the Message-Authenticator requirement or DTLS/RadSec support. The exploit requires an attacker to successfully Man-in-the-Middle (MITM) the RADIUS communication so if an attacker can't get onto a network segment with that traffic the attack is not possible. The reason this is only a partial mitigation is that a network misconfiguration or compromise of a portion of the network can expose the RADIUS traffic.

If RADIUS traffic can not be segmented or encrypted additional features can be implemented to prevent successful MITM on at risk segments such as: IP Source Guard, Dynamic ARP Inspection, and DHCP Snooping. It may also be possible to utilize other authentication methods based on the authentication flow type such as TACACS+, SAML, LDAPS, etc...

Identity Services Engine Vulnerability Status

The following tables describe what is available as of ISE 3.4 to make authentication flows protected against Blast-RADIUS. To recap, the following 3 items must be in plase for a flow utilizing only Message-Authenticator and not DTLS/RadSec/IPSec encryption, for the flow to not be vulnerable: 1) The Network Access Device MUST send the Message-Authenticator attribute in the Access-Request.

2) The RADIUS Server MUST require the Message-Authenticator attribute in the Access-Request.

3) The RADIUS Server MUST respond with the Message-Authenticator attribute in the Access-Challenge, Access-Accept, and Access-Reject.

Please refer to <u>CSCwk67747</u> which is tracking the changes to close the vulnerabilities when ISE is acting as the RADIUS client.

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

ISE as a RADIUS Server

ISE as a RADIUS Client

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