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 https://www.blastradius.fail/pdf/radius.pdf 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: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. 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. RFC 2869 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

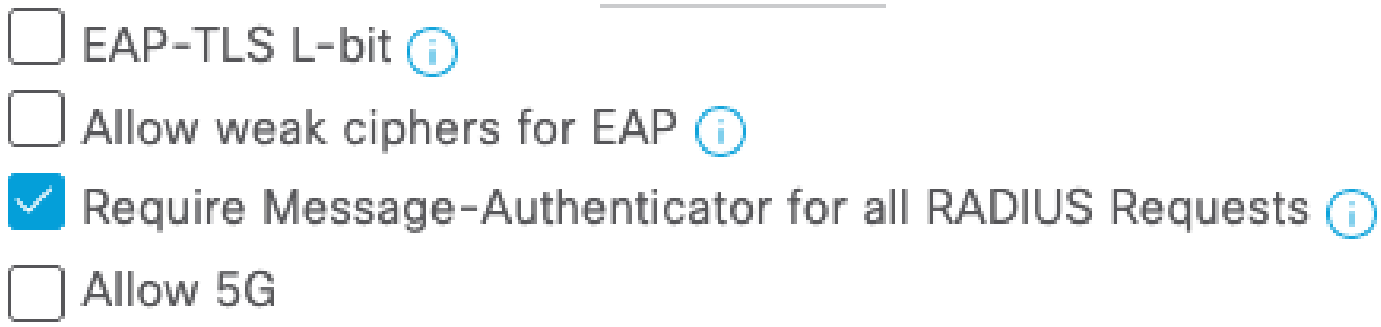
1) RADIUS client must include Message-Authenticator attribute.

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":



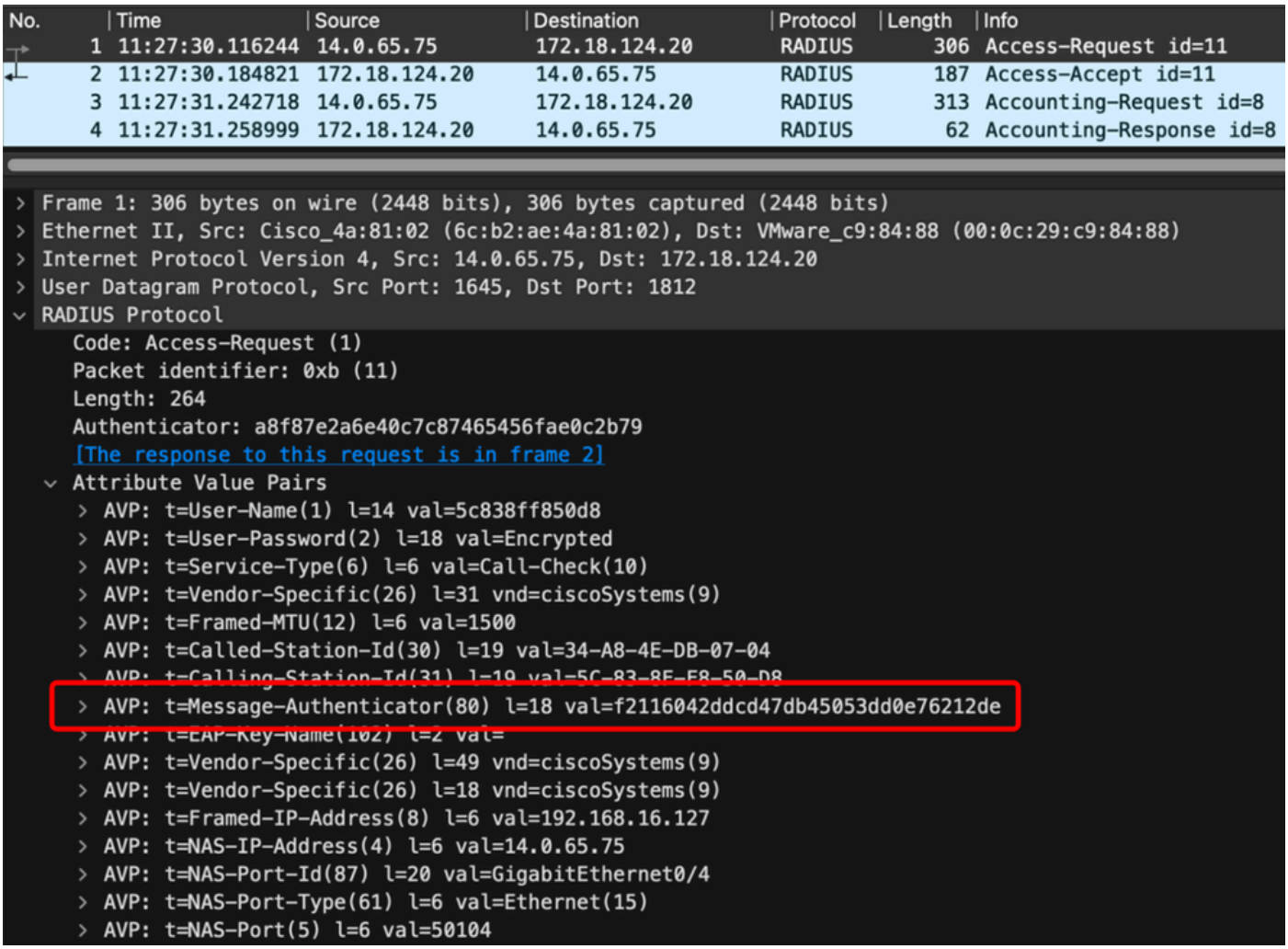
Allowed Protocols Option in Identity Services Engine

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

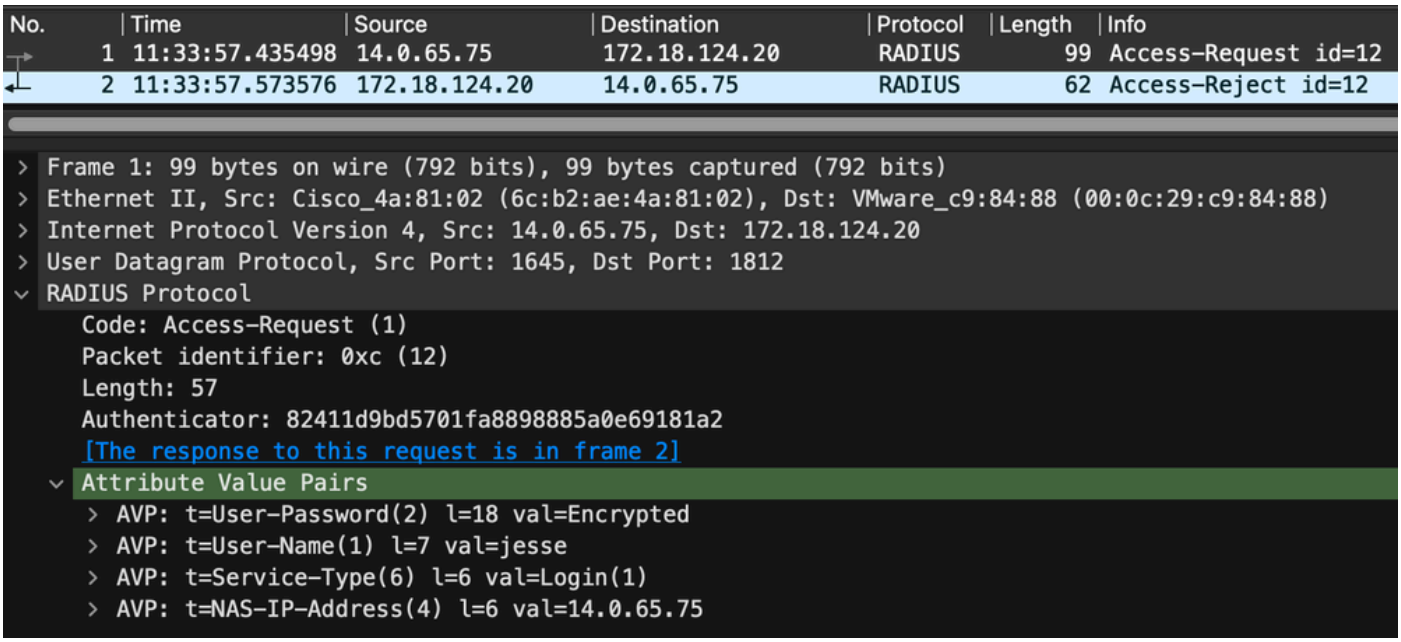
It is important to verify whether the NAD is sending Message-Authenticator before being require by the RADIUS Server as this is not a negotiated attribute, it is up to the NAD to send it either by default or be configured to send it. Message-Authenticator is not one of the attributes reported by ISE, 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:



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:



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 RFC 7360 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 RFC 6614, 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 mis-configuration 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 CSCwk67747 which is tracking the changes to close the vulnerabilities when ISE is acting as the RADIUS client.

ISE as a RADIUS Server

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 as a RADIUS Client

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