Blast-RADIUS(CVE-2024-3596) 프로토콜 스푸핑 완화

목차

소개

2024년 7월 7일, 보안 연구진은 RADIUS 프로토콜의 다음과 같은 취약성을 공개했습니다. CVE-2024-3596: RFC 2865의 RADIUS 프로토콜은 MD5 Response Authenticator 서명에 대해 선택된 접두사 충돌 공격을 사용하여 다른 임의의 응답에 대해 유효한 응답(Access-Accept, Access-Reject 또는 Access-Challenge)을 수정할 수 있는 경로 상의 공격자에 의한 위조 공격에 취약합니다. 이들은 https://www.blastradius.fail/pdf/radius.pdf에서 Message-Authenticator 특성을 사용하지 않는 흐름에 대해 성공적으로 응답을 위조했음을 입증하는 결과를 자세히 설명하는 논문을 발표했습니다.

이 취약성의 영향을 받는 Cisco 제품 및 수정 사항이 포함된 버전의 최신 목록을 보려면 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3을 방문하십시오. 이 문서에서는 일반적인 완화 기법과 일부 Cisco 제품에 적용되는 방법을 다룹니다. 단, 모든 Cisco 제품에 적용되는 것은 아닙니다. 자세한 내용은 개별 제품 설명서를 참조하십시오. Cisco의 주력 RADIUS 서버인 ISE(Identity Service Engine)에 대해 자세히 살펴보겠습니다.

배경

이 공격은 MD5의 충돌을 활용하는 MD5 선택 접두사 공격을 활용합니다. 그러면 공격자가 응답 패킷의 기존 특성을 수정하는 동시에 RADIUS 응답 패킷에 추가 데이터를 추가할 수 있습니다. RADIUS Access-Reject를 RADIUS Access-Accept로 변경하는 기능을 예로 들었습니다. 이는 RADIUS가 기본적으로 패킷에 있는 모든 특성의 해시를 포함하지 않기 때문에 가능합니다. RFC 2869는 Message-Authenticator 특성을 추가하지만 현재 EAP 프로토콜을 사용할 때만 포함하면 됩니다. 즉, RADIUS 클라이언트(NAD)에 Message-Authenticator 특성이 포함되지 않은 비 EAP 교환에 대해 CVE-2024-3596에 설명된 공격이 가능합니다.

완화

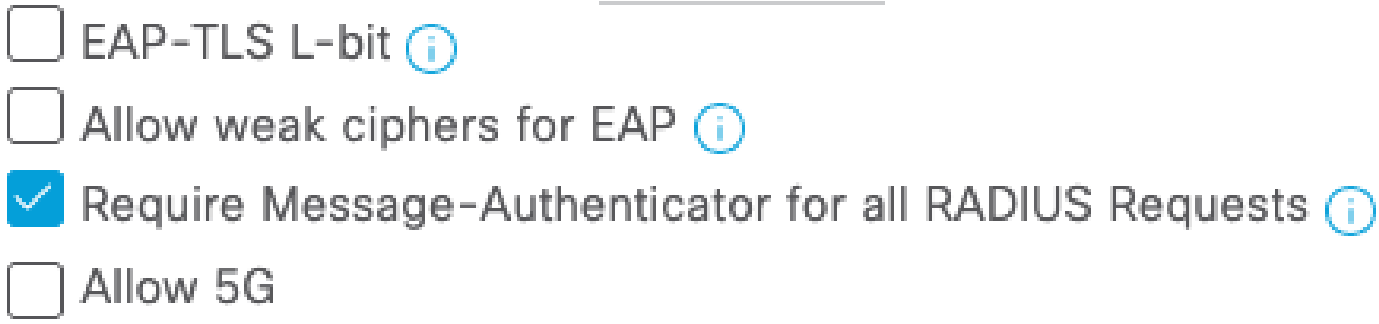
메시지 인증자

1) RADIUS 클라이언트는 메시지 인증자 특성을 포함해야 합니다.

네트워크 액세스 장치(NAD)가 액세스 요청에 메시지 인증자 특성을 포함하면 ISE(Identity Services Engine)는 모든 버전의 결과 Access-Accept, Access-Challenge 또는 Access-Reject 패킷에 메시지 인증자를 포함합니다.

2) RADIUS 서버는 메시지 인증자 특성의 수신을 적용해야 합니다.

공격은 RADIUS 서버로 전달되기 전에 메시지 인증자를 액세스 요청에서 제거할 수 있으므로 메시지 인증자를 액세스 요청에 포함시키는 것만으로는 충분하지 않습니다. 또한 RADIUS 서버는 NAD가 Access-Request에 Message-Authenticator를 포함하도록 해야 합니다. 이는 Identity Services Engine의 기본값이 아니지만 정책 설정 레벨에서 적용되는 허용되는 프로토콜 레벨에서 활성화할 수 있습니다. Allowed Protocols 컨피그레이션의 옵션은 "Require Message-Authenticator" for all RADIUS Requests"입니다.



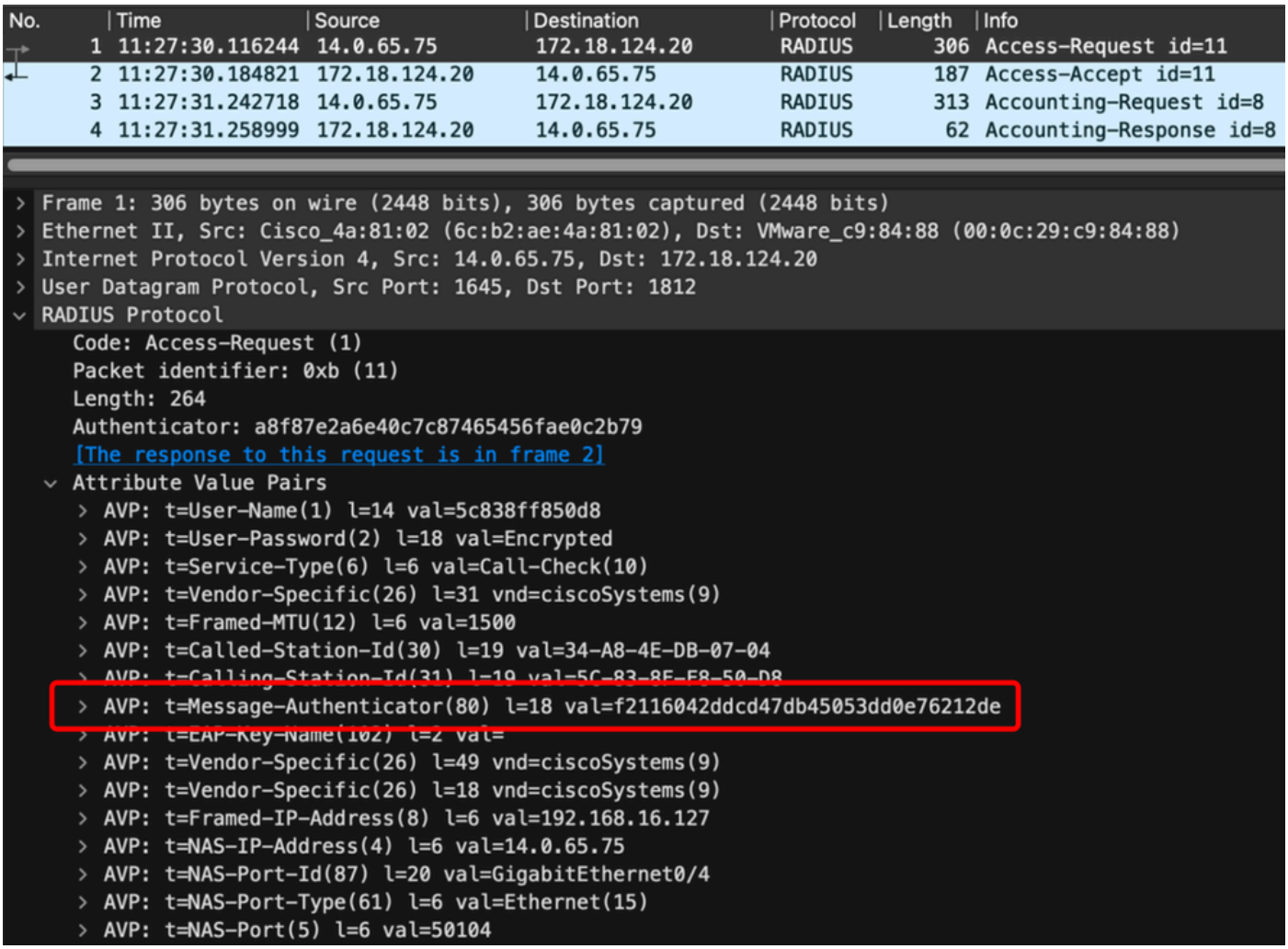
Identity Services Engine에서 허용되는 프로토콜 옵션

허용되는 프로토콜 컨피그레이션에 메시지 인증자가 필요하지만 액세스 요청에 메시지 인증자 특성이 포함되지 않은 정책 집합과 일치하는 인증은 ISE에서 삭제됩니다.

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

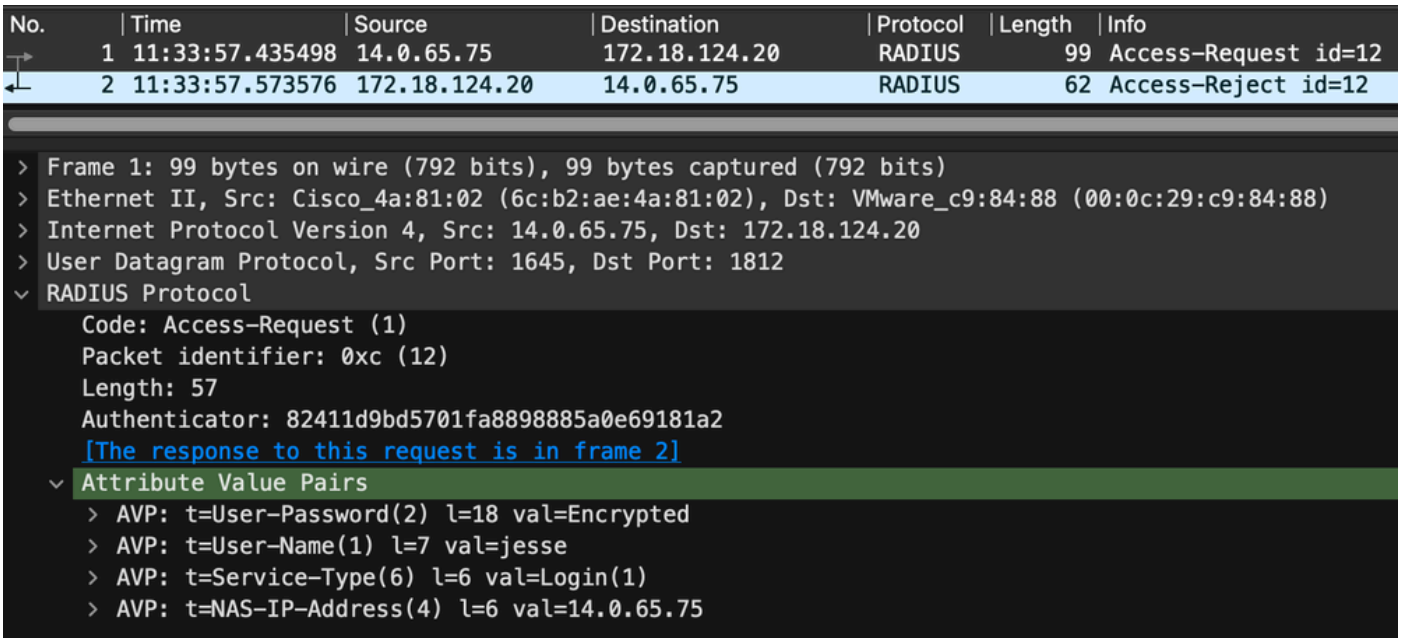
RADIUS 서버에 의해 요청되기 전에 NAD가 메시지 인증자를 전송하고 있는지 확인하는 것이 중요합니다. 이 특성은 협상된 특성이 아니며, 기본적으로 NAD에서 보내거나 보내도록 구성되어야 합니다. 메시지 인증자는 ISE에서 보고한 특성 중 하나가 아닙니다. 패킷 캡처는 NAD/활용 사례에 메시지 인증자가 포함되어 있는지 여부를 확인하는 가장 좋은 방법입니다. ISE는 Operations(운영) -> Troubleshoot(문제 해결) -> Diagnostic Tools(진단 도구) -> General Tools(일반 도구) -> TCP Dump(TCP 덤프)에 있는 패킷 캡처 기능을 기본적으로 제공합니다. 동일한 NAD의 다양한 활용 사례는 메시지 인증자를 포함하거나 포함하지 않을 수 있습니다.

다음은 Message-Authenticator 특성을 포함하는 Access-Request의 예제 캡처입니다.



Radius access-request의 message-authenticator 특성

다음은 Message-Authenticator 특성이 포함되지 않은 Access-Request의 예제 캡처입니다.



TLS/IPSec으로 암호화

RADIUS를 보호하는 가장 효과적인 장기 솔루션은 RADIUS 서버와 NAD 간의 트래픽을 암호화하는 것입니다. 이렇게 하면 MD5-HMAC 파생 메시지 인증자에만 의존하는 것보다 개인 정보 보호 기능과 더욱 강력한 암호화 무결성이 추가됩니다. RADIUS 서버와 NAD 간에 이 중 하나가 사용될 수 있는 경우 암호화 방법을 지원하는 양쪽에 따라 달라집니다.

RADIUS의 TLS 암호화를 위해 업계에서 사용되는 광범위한 용어는 다음과 같습니다.

- "RadSec" - RFC 6614를 나타냅니다.
- "RadSec TLS" - RFC 6614를 참조합니다.
- "RadSec DTLS" - RFC 7360을 참조합니다.

TLS 암호화에 대한 성능 오버헤드와 인증서 관리 고려 사항이 있으므로 제어 방식으로 암호화를 실행하는 것이 중요합니다. 인증서도 정기적으로 갱신해야 합니다.

RADIUS over DTLS

DTLS(Datagram Transport Layer Security)는 RADIUS를 위한 전송 레이어로 RFC 7360에 의해 정의됩니다. RFC는 인증서를 사용하여 RADIUS 서버를 상호 인증하고 NAD가 TLS 터널을 사용하여 전체 RADIUS 패킷을 암호화합니다. 전송 방법은 UDP로 유지되며 RADIUS 서버와 NAD 모두에 인증서를 구축해야 합니다. DTLS를 통해 RADIUS를 구축할 때는 만료된 인증서가 RADIUS 통신을 중단하지 않도록 인증서 만료 및 교체를 긴밀하게 관리해야 합니다. ISE는 ISE에서 NAD로의 통신을 위해 DTLS를 지원합니다. ISE 3.4부터 RADIUS over DTLS는 RADIUS 프록시 또는 RADIUS 토큰 서버에 대해 지원되지 않습니다. RADIUS over DTLS는 IOS-XE®를 실행하는 스위치 및 무선 컨트롤러와 같이 NAD로 작동하는 많은 Cisco 디바이스에서도 지원됩니다.

TLS를 통한 RADIUS

RFC 6614에 의해 RADIUS에 대한 TLS(Transport Layer Security) 암호화가 정의되며, TCP로의 전송을 변경하고 TLS를 사용하여 RADIUS 패킷을 완전히 암호화합니다. 이는 에듀롬 서비스가 그 예로 흔하게 사용하고 있다. ISE 3.4부터 RADIUS over TLS는 지원되지 않지만, IOS-XE를 실행하는 스위치 및 무선 컨트롤러와 같이 NAD로 작동하는 많은 Cisco 디바이스에서 지원됩니다.

IPSec

Identity Services Engine은 ISE와 NAD 간의 IPSec 터널에 대한 기본 지원을 제공하며 IPSec 터널 종료도 지원합니다. 이 옵션은 RADIUS over DTLS 또는 RADIUS over TLS가 지원되지 않지만 ISE 정책 서비스 노드당 150개의 터널만 지원되므로 적게 사용해야 하는 좋은 옵션입니다. ISE 3.3 이상에서는 더 이상 IPSec 라이센스가 필요하지 않으며, 이제 기본적으로 사용할 수 있습니다.

부분 완화

RADIUS 세그멘테이션

RADIUS 트래픽을 관리 VLAN으로 분할하고 SD-WAN 또는 MACSec을 통해 제공되는 것과 같은 암호화된 보안 링크를 제공합니다. 이러한 전략은 공격의 위험을 제로로 하는 것이 아니라 취약점의 공격 표면을 크게 줄일 수 있다. 이는 제품이 메시지 인증자 요구 사항 또는 DTLS/RadSec 지원

을 롤아웃하는 동안 적절한 MSS(Stop Gap Measure)일 수 있습니다. 공격자는 이 익스플로잇을 사용하여 RADIUS 통신을 MITM(Man-in-the-Middle)에 성공적으로 연결해야 합니다. 따라서 공격자가 해당 트래픽으로 네트워크 세그먼트에 도달할 수 없는 경우 공격을 수행할 수 없습니다. 이는 부분적인 완화에 불과한 이유는 네트워크가 잘못 구성되거나 네트워크 일부가 손상되면 RADIUS 트래픽이 노출될 수 있기 때문입니다.

RADIUS 트래픽을 분할할 수 없거나 암호화된 경우 IP Source Guard, Dynamic ARP Inspection 및 DHCP Snooping과 같은 위험 세그먼트에서 MITM이 성공하지 않도록 추가 기능을 구현할 수 있습니다. TACACS+, SAML, LDAPS 등과 같은 인증 흐름 유형에 따라 다른 인증 방법을 활용하는 것도 가능할 수 있다.

Identity Services Engine 취약성 상태

다음 표에서는 Blast-RADIUS에 대해 보호 된 인증 흐름을 만들기 위해 ISE 3.4에서 사용 할 수 있는 것에 대해 설명 합니다. 요약을 되풀이하려면 DTLS/RadSec/IPSec 암호화가 아닌 메시지 인증자만 사용하는 플로우에 대해 다음 3가지 항목이 있어야 합니다.
1) 네트워크 액세스 장치는 액세스 요청에서 메시지 인증자 특성을 전송해야 합니다.

2) RADIUS 서버는 Access-Request에 Message-Authenticator 특성을 요구해야 합니다.

3) RADIUS 서버는 Access-Challenge, Access-Accept 및 Access-Reject에서 Message-Authenticator 특성으로 응답해야 합니다.

ISE가 RADIUS 클라이언트로 작동할 때 취약성을 닫으려면 변경 사항을 추적하는 CSCwk67747을 참조하십시오.

RADIUS 서버로서의 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 클라이언트로 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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.