Blast-RADIUS (CVE-2024-3596) beperking van protocolspoofing

Inhoud

Inleiding

Op 7 juli 2024 hebben beveiligingsonderzoekers de volgende kwetsbaarheid in het RADIUS-protocol blootgelegd: CVE-2024-3596: RADIUS-protocol onder RFC 2865 is gevoelig voor vervalsingsaanvallen door een aanvaller op het pad die elke geldige Response (Access-Accept, Access-Reject of Access-Challenge) kan wijzigen naar een andere respons met behulp van een gekozen-prefix botsingsaanval tegen MD5 Response Authenticator-handtekening. Zij hebben een document gepubliceerd waarin hun bevindingen worden uiteengezet op https://www.blastradius.fail/pdf/radius.pdf dat een succesvolle reactie laat zien van vervalsing tegen stromen die geen gebruik maken van het kenmerk Message-Authenticator.

Voor een bijgewerkte lijst van Cisco-producten die door deze kwetsbaarheid zijn beïnvloed en versies die oplossingen bevatten, gaat u naar https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. Dit artikel biedt informatie over algemene onderdrukkingstechnieken en over de manier waarop deze van toepassing zijn op bepaalde, maar niet alle Cisco-producten. De afzonderlijke productdocumentatie moet worden geraadpleegd voor specificaties. Als vlaggenschip van Cisco RADIUS-server zal Identity Service Engine nader worden besproken.

Achtergrond

Deze aanval maakt gebruik van een MD5-voorvoegsel-aanval met behulp van botsingen in MD5, die een aanvaller in staat stelt om extra gegevens toe te voegen aan het RADIUS-reactiepakket terwijl bestaande kenmerken van het reactiepakket worden gewijzigd. Een voorbeeld dat werd gedemonstreerd, was de mogelijkheid om een RADIUS access-reject te wijzigen in een RADIUS access-acceptatie. Dit is mogelijk omdat RADIUS standaard geen hash van alle kenmerken in het pakket bevat. RFC 2869 voegt de eigenschap Message-Authenticator toe, maar het is momenteel alleen vereist om te worden opgenomen wanneer gebruik wordt gemaakt van EAP-protocollen, wat betekent dat de aanval beschreven in CVE-2024-3596 mogelijk is tegen elke niet-EAP-uitwisseling waarbij de RADIUS-client (NAD) niet de eigenschap Message-Authenticator bevat.

Beperken

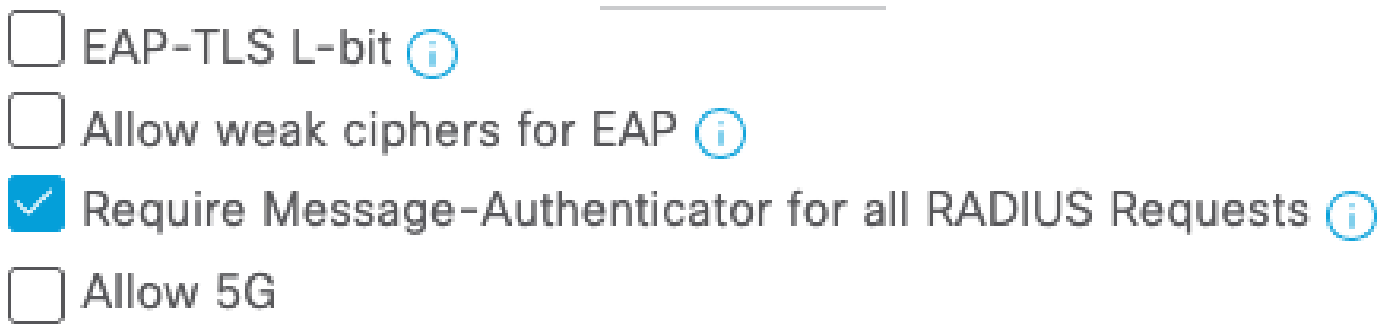
Berichtverificator

1) De RADIUS-client moet een kenmerk Message-Authenticator bevatten.

Wanneer het Network Access Device (NAD) het kenmerk Message-Authenticator in het toegangsverzoek bevat, zal Identity Services Engine in alle versies het resulterende pakket Access-Accept, Access-Challenge of Access-Reject omvatten.

2) De RADIUS-server moet het ontvangen van het kenmerk Message-Authenticator afdwingen.

Het is niet genoeg om alleen de Berichtverificator in het Toegang-Verzoek te omvatten aangezien de aanval het mogelijk maakt om de Berichtverificator van het Toegang-Verzoek te ontdoen alvorens het aan de Server van RADIUS wordt verstuurd. De RADIUS-server moet ook van de NAD eisen dat deze de Berichtverificator in het toegangsverzoek opneemt. Dit is niet standaard op Identity Services Engine maar kan worden ingeschakeld op het toegestane protocolniveau, dat van toepassing is op het beleidsniveau. De optie onder de configuratie Toegestane protocollen is "Require Message-Authenticator" voor alle RADIUS-aanvragen":



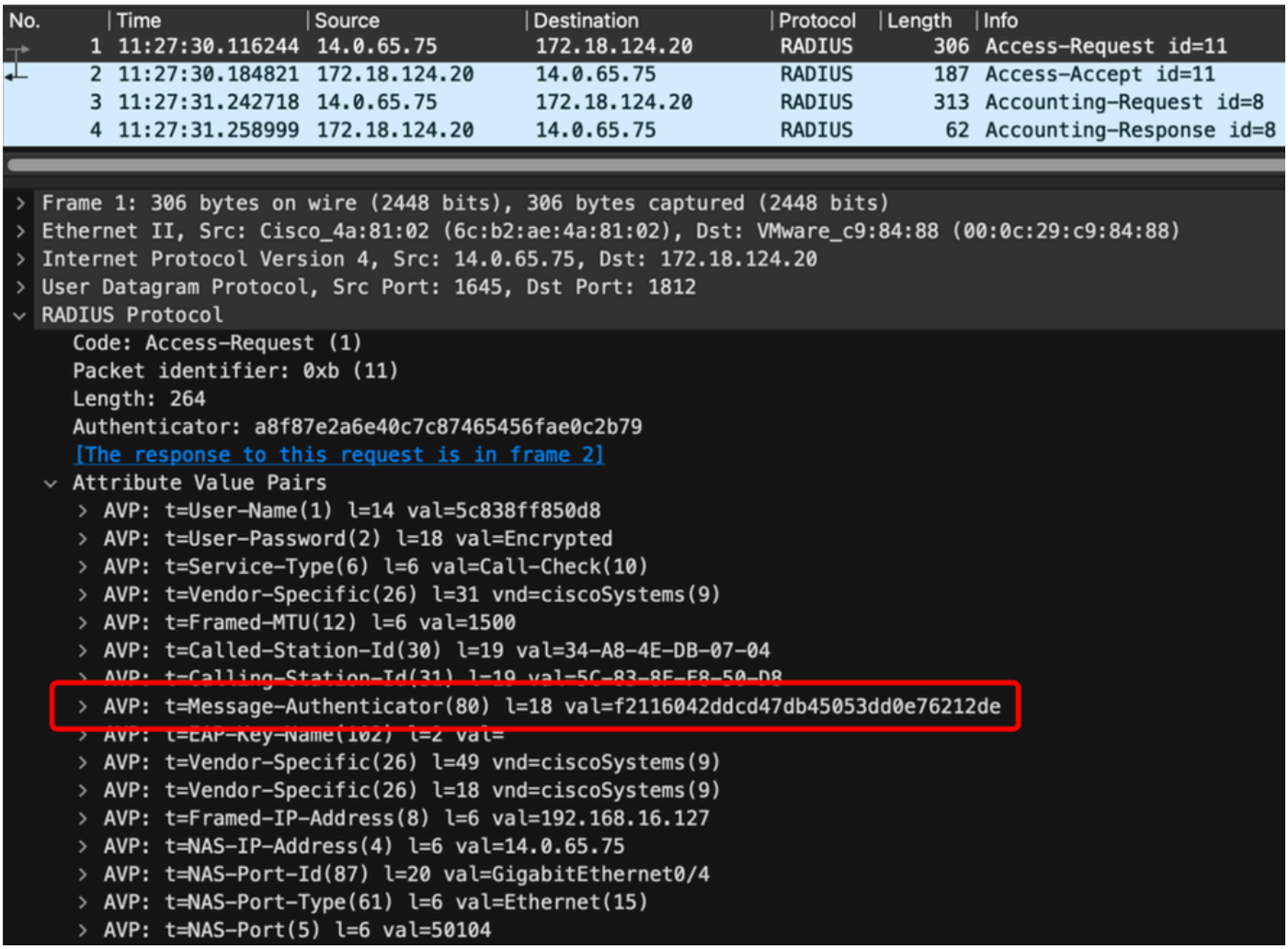
Toegestane protocoloptie in Identity Services Engine

Verificaties die overeenkomen met een beleidsset waarvoor de configuratie van Toegestane protocollen Message-Authenticator vereist, maar waarbij het Access-request geen Message-Authenticator-kenmerk bevat, worden door ISE gedropt:

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

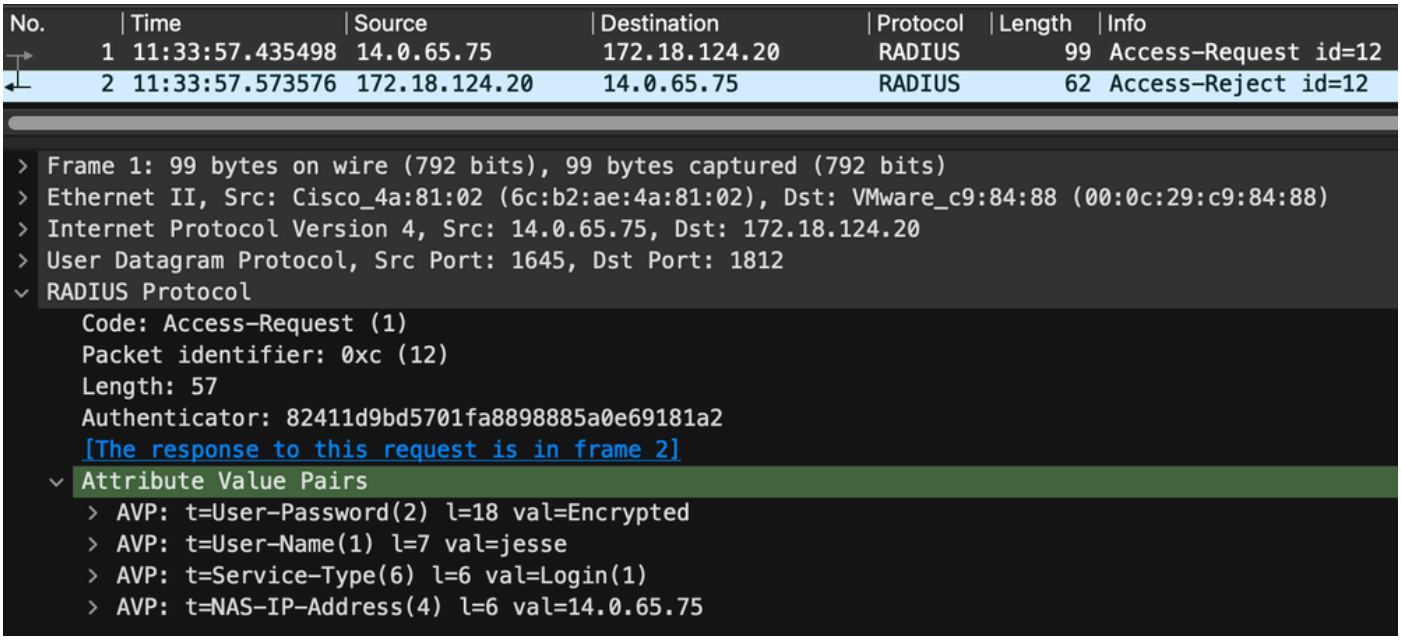
Het is belangrijk om te verifiëren of de NAD Berichtverificator verstuurt voordat deze door de RADIUS-server wordt vereist, aangezien dit geen onderhandelde eigenschap is, is het aan de NAD om het standaard te verzenden of geconfigureerd om het te verzenden. Message-Authenticator is geen kenmerk dat door ISE wordt gerapporteerd, maar een pakketopname is de beste manier om te bepalen of een NAD/Use Case een Message-Authenticator bevat. ISE heeft pakketopnamefuncties ingebouwd onder Operations -> Probleemoplossing -> Diagnostische tools -> Algemene tools -> TCP Dump. Houd in gedachten dat verschillende gebruikscases van dezelfde NAD kunnen of wel of niet Berichtverificator omvatten.

Het volgende is een voorbeeldopname van een access-request die het kenmerk Message-Authenticator bevat:



Berichtverificator-kenmerk in RADIUS-toegangsverzoek

Het volgende is een voorbeeldopname van een access-request die niet het kenmerk Message-Authenticator bevat:



Versleutelen met TLS/IPSec

De meest effectieve langetermijnoplossing om RADIUS te beveiligen is het verkeer tussen de RADIUS-server en het NAD te versleutelen. Dit voegt zowel privacy als sterkere cryptografische integriteit toe door alleen te vertrouwen op de MD5-HMAC afgeleide Message-Authenticator. Welke, als een van deze kan worden gebruikt tussen de RADIUS-server en de NAD, is afhankelijk van beide kanten die de coderingsmethode ondersteunen.

De algemene termen die in de branche worden gebruikt voor TLS-encryptie van RADIUS zijn:

- "RadSec" - verwijst naar RFC 6614
- "RadSec TLS" - verwijst naar RFC 6614
- "RadSec DTLS" - verwijst naar RFC 7360

Het is belangrijk om encryptie op een gecontroleerde manier uit te rollen aangezien er prestatiesoverheadkosten aan TLS encryptie evenals overwegingen van het certificaatbeheer zijn. Ook zullen de certificaten regelmatig moeten worden verlengd.

RADIUS via DTLS

Datagram Transport Layer Security (DTLS) als een transportlaag voor RADIUS is gedefinieerd door RFC 7360 die certificaten gebruikt om de RADIUS-server en het NAD wederzijds te authenticeren en vervolgens het volledige RADIUS-pakket te versleutelen met een TLS-tunnel. De transportmethode blijft UDP en vereist dat certificaten worden geïmplementeerd op zowel de RADIUS-server als de NAD. Houd in gedachten dat wanneer u RADIUS via DTLS implementeert, het absoluut noodzakelijk is dat het verlopen en de vervanging van het certificaat nauw worden beheerd om te voorkomen dat verlopen certificaten de RADIUS-communicatie onderbreken. ISE ondersteunt DTLS voor ISE-naar-NAD communicatie, vanaf ISE 3.4 Radius via DTLS wordt niet ondersteund voor RADIUS-Proxy of RADIUS-Token servers. RADIUS over DTLS wordt ook ondersteund door veel Cisco-apparaten die fungeren als NAD's, zoals switches en draadloze controllers waarop IOS-XE® wordt uitgevoerd.

RADIUS via TLS

Transport Layer Security (TLS) Encryptie voor RADIUS wordt gedefinieerd door RFC 6614, wijzigt het transport in TCP en gebruikt TLS om RADIUS-pakketten volledig te versleutelen. Dit wordt vaak gebruikt door de reduroamdienst als voorbeeld. Vanaf ISE 3.4 wordt RADIUS via TLS niet ondersteund, maar ondersteund door veel Cisco-apparaten die fungeren als NAD's, zoals switches en draadloze controllers met IOS-XE.

IPSEC

Identity Services Engine heeft native ondersteuning voor IPSec-tunnels tussen ISE en NAD's die ook ondersteuning bieden voor het beëindigen van IPSec-tunnels. Dit is een goede optie waarbij RADIUS via DTLS of RADIUS via TLS niet wordt ondersteund, maar spaarzaam moet worden gebruikt, aangezien slechts 150 tunnels worden ondersteund per knooppunt voor ISE-beleidsservices. ISE 3.3 en later geen licentie meer nodig voor IPSec, is nu standaard beschikbaar.

Gedeeltelijke beperking

RADIUS-segmentering

Segmenteer RADIUS-verkeer naar beheer-VLAN's en beveiligde, versleutelde koppelingen zoals die kunnen worden geboden via SD-WAN of MACSec. Deze strategie brengt het risico van de aanval niet tot nul, maar kan het aanvalsoppervlak van de kwetsbaarheid aanzienlijk verminderen. Dit kan een goede stop gap maatregel zijn terwijl de producten de eis van de Bericht-Authenticator of steun DTLS/RadSec uitrollen. De exploit vereist een aanvaller om met succes Man-in-the-Middle (MITM) de RADIUS-communicatie, zodat als een aanvaller niet op een netwerksegment kan komen met dat verkeer, de aanval niet mogelijk is. De reden dat dit slechts een gedeeltelijke matiging is is dat een netwerk fout-configuratie of compromis van een gedeelte van het netwerk het verkeer van de RADIUS kan blootstellen.

Als RADIUS-verkeer niet kan worden gesegmenteerd of versleuteld, kunnen aanvullende functies worden geïmplementeerd om succesvolle MITM op risicosegmenten te voorkomen, zoals IP Source Guard, Dynamic ARP Inspection en DHCP-controle. Het kan ook mogelijk zijn andere verificatiemethoden te gebruiken die zijn gebaseerd op het type verificatiestroom, zoals TACACS+, SAML, LDAPS, enz...

Kwetsbaarheidsstatus voor Identity Services Engine

In de volgende tabellen wordt beschreven wat er beschikbaar is vanaf ISE 3.4 om verificatiestromen te beschermen tegen Blast-RADIUS. Om samen te vatten, moeten de volgende 3 punten in plaats van een stroom zijn die slechts bericht-Authenticator en niet encryptie DTLS/RadSec/IPSec gebruikt, voor de stroom om niet kwetsbaar te zijn:
1) Het netwerktoegangsapparaat MOET het kenmerk Message-Authenticator in het toegangsverzoek verzenden.

2) De RADIUS-server MOET het kenmerk Message-Authenticator in het toegangsverzoek vereisen.

3) De RADIUS-server MOET reageren met het kenmerk Message-Authenticator in de bestandsuitdaging, toegangsaanvaarding en toegangsweigering.

Raadpleeg CSCwk67747 die de wijzigingen bijhoudt om de kwetsbaarheden te sluiten wanneer ISE als RADIUS-client optreedt.

ISE als 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 als 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.