

Secure Access RA VPN-verificatie-evenementen met Link-Local AAA-serveradressen

Inhoud

uitgifte

Bij het testen van de Secure Access Remote Access (RA) VPN-functionaliteit worden buitensporige verificatiegebeurtenissen vastgelegd voor identiteiten die niet bestaan in de tenantorganisatie. De verificatielogboeken tonen meer dan 10.000 RA VPN-verificatiegebeurtenissen binnen een periode van 24 uur, met AAA-fouten zoals "AALOG_SERVICE_DOWN" en "AALOG_SERVER_DOWN". Deze foutmeldingen verwijzen naar link-local 169.254.x.x adressen als de AAA-server, die niet zijn geconfigureerd in de huurder.

Specifieke voorbeelden van fouten die in de logbestanden zijn waargenomen, zijn:

```
AAALOG_SERVICE_DOWN  
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>
```

```
AAALOG_SERVER_DOWN  
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

De activiteit lijkt te worden herhaald op RADIUS gebaseerde authenticatie pogingen tegen de Secure Access VPN FQDN, het creëren van overmatige log ruis en het verhogen van de bezorgdheid over externe scanning of mogelijk misbruik van de VPN-service.

milieu

- Cisco Secure Access-platform
- VPN-profiel voor externe toegang aanvankelijk geconfigureerd zonder certificaatverificatie
- Op RADIUS gebaseerde verificatie geconfigureerd voor RA VPN

- Openbare VPN-tenantconfiguratie met vindbare VPN-profielen

resolutie

De resolutie omvatte het begrijpen van het authenticatiestroom-gedrag en het implementeren van op certificaten gebaseerde authenticatie als een mitigatiestrategie.

Technische verklaring van waargenomen gedrag

De excessieve authenticatie-gebeurtenissen treden op vanwege de technische redenen die in de volgende secties worden beschreven.

Verificatiestroom zonder certificaatvereisten

Wanneer certificaatverificatie is uitgeschakeld en RADIUS-gebaseerde RA VPN-verificatie wordt gebruikt, registreert het systeem "mislukte autorisatiepogingen" omdat het systeem eerst de gebruikersnaam en identiteit controleert aan de hand van de database van gebruikers die zijn gesynchroniseerd in Secure Access en de gebeurtenis "mislukte autorisatie" registreert. Deze gebeurtenissen worden verwacht als een eerste verdedigingslinie, maar kunnen aanzienlijke logruis produceren wanneer externe actoren authenticatie proberen.

Link-lokaal adresgebruik

De 169.254.x.x-adressen die in logs worden weergegeven, zijn interne / lokale verbindingsadressen die door de RA VPN-kop worden gebruikt om inkomende sessies te autoriseren. Deze adressen vertegenwoordigen intern systeemgedrag in plaats van een verkeerde configuratie van AAA-servers in de tenant.

VPN-profieldetectie

Wanneer een openbare VPN-tenant-ID is geconfigureerd, worden de VPN-profielen vermeld in de UI-vervolgkeuzelijst, waarmee externe actoren openbare profielen gemakkelijker kunnen ontdekken en deze kunnen targeten voor verificatiepogingen.

Onmiddellijke mitigatiestappen

1.- Certificaatgebaseerde verificatie configureren. Wijzig het RA VPN-profiel om op certificaten gebaseerde verificatie te vereisen. Wanneer certificaatverificatie vereist is, voert Secure Access eerder in de verificatiestroom een certificaatcontrole uit. Als het certificaat ontbreekt, produceert het systeem een fout vóór de standaard verificatiestroom en worden de gebeurtenissen met betrekking tot "mislukte autorisatie" niet op dezelfde manier geregistreerd.

2.- De doeltreffendheid van mitigatie valideren. Controleer de verificatielogboeken na het implementeren van op certificaten gebaseerde verificatie om de vermindering van buitensporige verificatiegebeurtenissen te bevestigen. Door over te schakelen op certificaatgebaseerde verificatie konden de aanvallen met succes worden beperkt en werd de logruis verminderd.

Verbeteringen op lange termijn

Er zijn twee functieverzoeken gemaakt om de onderliggende problemen aan te pakken:

- Functieaanvraag 1: Voeg een optie toe om de lijst met tunnelgroepen (VPN-profiel) te verbergen of weer te geven wanneer een openbare VPN-tenant wordt toegevoegd, waardoor de profielvindbaarheid wordt verminderd.
- Functieverzoek 2: Voeg een configuratieoptie toe om logboekregistratie van mislukte RA VPN-autorisatiepogingen in of uit te schakelen, waardoor beheerders controle hebben over de logboeksnelheid.

Daarnaast wordt een document met een openbare weergave gemaakt om de gebeurtenissen en het verificatiegedrag in de logboekregistratie uit te leggen, zodat beheerders de normale systeembewerkingen beter kunnen begrijpen.

Oorzaak

De hoofdoorzaak van de buitensporige authenticatie-gebeurtenissen is de combinatie van detecteerbare VPN-profielen in openbare tenantconfiguraties en het verificatiestroom-gedrag wanneer op certificaten gebaseerde authenticatie niet vereist is. Wanneer op RADIUS gebaseerde authenticatie wordt gebruikt zonder certificaatvereisten, registreert het systeem alle "mislukte autorisatiepogingen" als onderdeel van zijn beveiligingspositie, inclusief pogingen van externe actoren die de VPN-profielen ontdekken. De link-lokale adressen in de logs vertegenwoordigen normaal intern systeemgedrag voor het RA VPN headend autorisatieproces, geen configuratiefouten.

Gerelateerde inhoud

- [Cisco Technical Support en downloads](#)

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.