

ISE Admin GUI Login mislukt met PingID Federation RADIUS Token

Inhoud

uitgifte

De aanmelding van de GUI van de beheerder bij Cisco ISE mislukt wanneer de PingID-federatie wordt gebruikt als een RADIUS-token, ondanks dat pakketopnamen aantonen dat Ping Federate een Access-Accept-antwoord retourneert. De aanmeldingsfout treedt op, ook al lijkt de RADIUS-verificatie succesvol vanuit netwerkperspectief, waardoor de toegang van de beheerder tot de ISE-interface wordt verhinderd. Netwerkpakketanalyse bevestigt dat de PingID-server (10.32.154.200) het verwachte Access-Accept-antwoord naar ISE (10.2.200.241) verzendt, maar het ISE-beheerdersaanmeldingsproces is nog steeds niet voltooid.

milieu

- Cisco Identity Services Engine (ISE) versie 3.3 Patch 7
- VM-implementatie met 4 knooppunten
- PingID-federatie geconfigureerd als RADIUS-tokenverificatie
- ISE IP-adres: 10.2.200.241
- IP-adres PingID-server: 10.32.154.200
- Beheerderstoegangsconfiguratie beoordeeld onder Beheer > Beheerderstoegang

resolutie

Het probleem werd opgelost door de toepassing van een tijdelijke oplossing die een succesvolle aanmeldingsfunctionaliteit voor beheerders mogelijk maakte. De stappen die in de volgende

paragrafen worden beschreven, zijn genomen om het probleem aan te pakken.

Stap 1: Verzamelen en analyseren van bewijsmateriaal

Er is pakketregistratiebewijs verzameld en geanalyseerd om de RADIUS-verificatiestroom tussen ISE en de PingID-server te bevestigen. De analyse verifieerde dat Ping Federate correct Access-Accept-antwoorden verstuurde.

Stap 2: Bewijs van prrt-server.log

###

prrt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

Stap 3: Wat is een Message Authenticator?

De Message-Authenticator is een beveiligingsattribuut dat wordt gebruikt in RADIUS-pakketten om de integriteit en authenticiteit van de berichten die worden uitgewisseld tussen netwerkkapparaten en de RADIUS-server te garanderen. Het is een cryptografische handtekening die wordt berekend met behulp van HMAC-MD5 over het hele RADIUS-pakket met een gedeelde geheime sleutel. Deze eigenschap helpt u te beschermen tegen manipulatie en vervalsing van RADIUS-berichten, met name die met Extensible Authentication Protocol (EAP)-verificatiestromen.

Stap 4: Implementatie van workaround

Schakel "Message Authenticator Required On Response" (Berichtenverificator vereist bij reactie) uit: Administratie / Identiteitsbeheer / Externe identiteitsbronnen / RADIUS-token. Klik op de naam van het RADIUS-token en ga vervolgens naar Verificatie. Schakel het selectievakje "Message Authenticator required on response" (Berichtenverificator vereist bij reactie) uit.

Stap 5: Validatie testen

Na het toepassen van de workaround werden admin login tests uitgevoerd om de resolutie te valideren. Deze tests bevestigden succesvolle authenticatie en toegang tot de ISE-beheerdersinterface met PingID-federatie als het RADIUS-token.

Stap 6: Monitoringsperiode

Er werd een monitoring-en validatieperiode vastgesteld om de stabiliteit van de workaround te waarborgen. Gedurende deze periode werd doorgegaan met het testen van de admin-login zonder dat fouten of storingen werden gemeld.

Oorzaak

De ISE Admin GUI-aanmeldingsfout werd veroorzaakt door een discrepantie tussen Cisco ISE 3.3 Patch 7 en PingID (Ping Federate) tijdens MFA-verificatie.

Concreet:

- Cisco ISE vereiste dat het RADIUS Message-Authenticator-kenmerk aanwezig moest zijn in de Access-Accept-respons van de externe RADIUS-tokenserver.
- PingID retourneerde Access-Accept-antwoorden zonder het Message-Authenticator-attribuut.
- Omdat ISE de instelling Message Authenticator Required On Response ingeschakeld had, verwierp het in stilte de RADIUS-respons als ongeldig, ook al is de verificatie zelf geslaagd aan de PingID-kant.
- Deze handhaving maakt deel uit van de beveiligingshardening van Cisco ISE om de kwetsbaarheid van Blast-RADIUS (CVE-2024-3596) te beperken.

Gerelateerde inhoud

- [Beperking van spoofing door explosiestralen \(CVE-2024-3596\)](#)

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.