Secure Access Certificate Inspection Posture Check-verificatiefouten

Inhoud

uitgeven

Wanneer u probeert om Secure Access te implementeren met het Endpoint-houdingsprofiel met behulp van de functie voor certificaatinspectie, mislukken alle aanmeldingspogingen, ondanks het feit dat specifieke oorzaken van fouten niet kunnen worden geïdentificeerd in de DART-bundellogs.Gebruikers proberen SAML IDP-verificatie te gebruiken terwijl ze ook certificaatvalidatie willen afdwingen via het mechanisme voor houdingscontrole, maar deze configuratie resulteert in consistente verificatiefouten, zelfs wanneer back-endcertificaatovereenkomsten succesvol zijn.

milieu

- Cisco Secure Access - beveiligde externe clienttoegang (VPN, houding, privébron)
- Integratie van SAML IDP-verificatie
- Eindpunthoudingsprofiel met functie voor certificaatinspectie ingeschakeld
- Gebruikerscertificaten met UPN-veld in overeenkomende SAN-e-mailadressen
- Beveiligde toegang tot tenant-configuratie met gebruikers, groepen en eindpuntapparaten

resolutie

De eindpuntcontroles voor certificaten in postuur worden alleen afgedwongen bij het gebruik van meervoudige certificaatverificatie, waarvoor zowel een gebruikerscertificaat als machinecertificaatvalidatie vereist is. Aangezien het implementatiescenario gebruikers omvat met alleen gebruikerscertificaten die één VPN-profiel moeten gebruiken, omvat de oplossing de

implementatie van SAML + Single-certificaatverificatie in plaats van te vertrouwen op posture-certificaatcontrole.

Configuratiestappen voor verificatie

Stap 1: SAML + Single Certificate Authentication configureren

Configureer de verificatiemethode voor het gebruik van SAML-verificatie in combinatie met enkelvoudige certificaatverificatie in plaats van te proberen certificaatvalidatie af te dwingen door middel van houdingscontroles.

Stap 2: Certificaat UPN-overeenkomst configureren

Zorg ervoor dat het veld UPN in de alternatieve onderwerpnaam (SAN) van het certificaat het e-mailadres van de gebruiker bevat dat overeenkomt met de eigenschap auth die is geconfigureerd voor de gebruiker in Secure Access onder Gebruikers, Groepen en Eindpuntapparaten.

Stap 3: Primair verificatieveld instellen

Configureer het primaire veld voor verificatie met behulp van de UPN van het certificaat en zorg ervoor dat het overeenkomt met het e-mailadres van de gebruiker in de gebruikersdatabase voor beveiligde toegang.

Vereisten voor de certificaatstructuur

De certificaatstructuur moet zo worden geconfigureerd dat de UPN- of secundaire waarde in het certificaat overeenkomt met de eigenschap auth voor de gebruiker in Secure Access. Als een gebruiker een certificaat presenteert met een UPN- of secundaire waarde die niet overeenkomt met de geconfigureerde eigenschap auth voor die gebruiker in Secure Access, wordt de verificatie afgewezen.

Belangrijke opmerkingen over de configuratie

Multi-certificaatverificatie (IDP SAML + Multi-Cert Auth) zou vereist zijn als handhaving van de

posture-certificaatcontrole nodig is, maar dit vereist zowel gebruikers- als machinecertificaten. Voor implementaties waarbij gebruikers alleen gebruikerscertificaten hebben en één VPN-profiel moeten gebruiken, biedt SAML + Single Certificate Authentication de juiste oplossing met behoud van op certificaten gebaseerde beveiligingscontroles.

Oorzaak

De eindpuntcontroles voor certificaten in postuur worden alleen afgedwongen wanneer verificatie met meerdere certificaten is geconfigureerd. Bij het gebruik van SAML-verificatie met posture-certificaatcontrole verwacht het systeem dat zowel gebruikers- als machinecertificaten aanwezig zijn voor validatie. Aangezien de implementatie alleen gebruikmaakte van gebruikerscertificaten met SAML-verificatie, mislukte de functie voor posture-certificaatinspectie consequent in verificatiepogingen, ondanks succesvolle back-end-certificaatmatching, omdat het posture-mechanisme niet was ontworpen om te werken met enkelvoudige certificaatverificatiescenario's.

Verwante 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.