Secure Access ZTNA RDP Private Resource Access-fout voor één specifieke bron

Inhoud

uitgifte

Gebruikers konden geen toegang krijgen tot één specifieke RDP-privébron via Cisco Secure Access Zero Trust Network Access (ZTNA). Wanneer gebruikers proberen verbinding te maken, ontvangen ze een bericht "interne fout opgetreden". Het probleem had gevolgen voor meerdere gebruikers, waaronder nieuw toegevoegde gebruikers, en voorkwam dat thuiswerkers toegang hadden tot de vereiste desktopbronnen. Andere POP-middelen en niet-POP-particuliere middelen bleven toegankelijk, wat erop wijst dat het probleem specifiek was voor deze specifieke middelenconfiguratie.

milieu

- Cisco Secure Access - Zero Trust Network Access (ZTNA)
- Configuratie van privébronnen met RDP-protocol
- Active Directory (AD)-groepsgebaseerd toegangsbeleid
- Meerdere configuraties van privébronnen met overlappende IP-adressen
- Klantgebaseerde inschrijving en postuur beoordeling

resolutie

Het probleem is opgelost door configuratieconflicten te identificeren en te corrigeren in de configuratie van de privébron. De stappen die in de volgende secties worden beschreven, zijn genomen om het probleem op te lossen.

Configuratieconflicten identificeren

Uit onderzoek is gebleken dat de specifieke RDP-bron is geconfigureerd onder meerdere privébronnen: Aanmelden bij CSA Dashboard > Verbinden > Eindgebruikersconnectiviteit > Onder Zero Trust Access > Een ZTA-profiel toevoegen > Een naam geven, en vervolgens zoeken naar een specifieke bestemming.

Conflicterende IP-adrestoewijzingen verwijderen

Het IP-adres 172.26.106.136 is verwijderd uit conflicterende privébronnen.

Het IP-adres is alleen achtergelaten onder de juiste bron die overeenkomt met de Active Directory-groepslidmaatschappen van de gebruikers en de vereisten voor het toegangsbeleid.

Gebruikersgroeplidmaatschap verifiëren

Er werd bevestigd dat nieuw toegevoegde gebruikers die problemen met de toegang ondervonden, geen lid waren van de juiste Active Directory (AD)-groep die vereist is voor toegang volgens het geconfigureerde toegangsbeleid.

Zorg er ook voor dat de juiste AD-groep of -gebruiker is gekoppeld aan het toegangsprofiel Zero Trust.

Toegang testen na wijzigingen in configuratie

Nadat de configuratiewijzigingen waren geïmplementeerd, konden gebruikers met succes toegang krijgen tot de RDP-resource zoals vereist. Er werd bevestigd dat het probleem was opgelost en dat gebruikers verbinding konden maken zonder het bericht "interne fout opgetreden" te ontvangen.

Oorzaak

De hoofdoorzaak van het probleem was een configuratieconflict waarbij de specifieke resource werd toegewezen aan meerdere privébronnen met verschillende toegangsbeleidsregels. Dit creëerde een situatie waarin gebruikers werden beoordeeld aan de hand van beleid waarvoor ze niet het juiste Active Directory-groepslidmaatschap hadden, wat resulteerde in toegangsweigeringen en het bericht "interne fout opgetreden". De nieuw toegevoegde gebruikers waren geen lid van de juiste AD-groepen die nodig zijn voor het conflicterende beleid, waardoor ze geen toegang hadden tot de bron, hoewel ze toegang moesten hebben gehad via het juiste beleid.

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.