Verbindingsproblemen met Cowork (Frontier) Agent oplossen wanneer Umbrella is ingeschakeld

Inhoud

uitgifte

De Cowork (Frontier)-agent werkte niet goed op laptops toen Cisco Umbrella was ingeschakeld. Toen Cisco Umbrella inactief was, functioneerde de agent zoals verwacht. Gebruikers konden de Cowork-agentfunctionaliteit niet gebruiken toen Umbrella actief was en er waren geen bloklogs zichtbaar in Cisco Umbrella toen gebruikers dit probleem ondervonden. Er werden foutscreenshots verstrekt waarop de toepassingsfouten tijdens de werking van Umbrella worden weergegeven.

milieu

- Cisco Umbrella geïmplementeerd op zakelijke laptops
- Cowork (Frontier) agent applicatie
- SSL/TLS-verkeersinspectie ingeschakeld in Cisco Umbrella
- Certificaatvastzetten geïmplementeerd in de Cowork-toepassing

resolutie

Het probleem werd opgelost door de Cowork-applicatie toe te voegen aan de Do Not Decrypt (DND)-lijst in Cisco Umbrella. Met deze configuratiewijziging kan de Cowork-agent SSL/TLS-inspectie omzeilen en zijn directe gecodeerde verbinding met de Cowork-servers onderhouden.

Stappen om DND-lijst te configureren

Stap 1: Open het Cisco Umbrella-dashboard en navigeer naar de SSL-decoderingsbeleidsconfiguratie.

Stap 2: Voeg Cowork-gerelateerde domeinen en URL's toe aan de lijst Niet decoderen om SSL-inspectie voor deze toepassing te omzeilen.

Stap 3: Pas de beleidswijzigingen toe en geef de configuratie de tijd om zich naar alle eindpunten te verspreiden.

Stap 4: Test de Cowork-agentfunctionaliteit met Cisco Umbrella ingeschakeld om de juiste werking te controleren.

validering

Nadat de DND-lijstconfiguratie was geïmplementeerd, functioneerde de Cowork-toepassing normaal met Cisco Umbrella ingeschakeld. Interne tests bevestigden dat het probleem zich niet opnieuw voordeed gedurende meerdere dagen van monitoring en alle gebruikers hadden toegang tot de Cowork-functionaliteit zoals verwacht.

Oorzaak

De Cowork (Frontier)-agent gebruikt het vastzetten van certificaten als beveiligingsmechanisme. Certificaatvastzetten betekent dat de toepassing is gehardcodeerd om alleen zijn eigen specifieke servercertificaat te accepteren en te vertrouwen. Wanneer Cisco Umbrella het verkeer onderschept en het Cisco-certificaat presenteert in plaats van het oorspronkelijke servercertificaat, detecteert de Cowork-toepassing deze wijziging, gaat ervan uit dat de verbinding niet veilig is en laat de verbinding opzettelijk vallen om de gegevens te beschermen. Dit wordt verwacht voor toepassingen die beveiligingsmaatregelen voor het vastzetten van certificaten implementeren.

Gerelateerde inhoud

- Effectieve niet-ontsleutelingslijst voor Microsoft-toepassingen maken
- 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.