

Problemen met de VPN-connectiviteit van de beveiligde client bij defecte postuur-detectie

Inhoud

uitgifte

Gebruikers kunnen geen Cisco Secure Client VPN-verbinding tot stand brengen in een Windows 365 VDI-omgeving of lokale pc's. De VPN-verbinding faalt consequent met houdingsgerelateerde fouten, met name het weergeven van "hostscan csd vooraanmelding verificatie mislukt" foutmeldingen.

Het probleem is geïdentificeerd als geassocieerd met posture detectie mislukt wanneer gebruikersnamen niet-ASCII (2-byte) tekens bevatten, waardoor getroffen VDI-gebruikers geen verbinding kunnen maken met de VPN.

Wanneer gebruikers op de verbindingstoets in de Cisco Secure Client-interface drukken, mislukt de VPN-verbinding. De fout manifesteert zich tijdens de fase van de postuur-evaluatie van het verbindingsproces, waardoor gebruikers geen veilige externe toegang tot bedrijfsbronnen via de VPN-tunnel tot stand kunnen brengen.

milieu

- Windows 365 VDI-omgeving of lokale pc
- Cisco Secure Client geïnstalleerd
- Secure Access-implementatie: RAVPN

resolutie

Dit probleem wordt momenteel onderzocht door Cisco Engineering en wordt gevolgd onder Cisco bug ID CSCwt59834. Het probleem komt voort uit fouten in de houdingsdetectie wanneer gebruikersnamen niet-ASCII (2-byte) tekens bevatten in de Windows 365 VDI-omgeving.

Date : 03/03/2026|Time : 02:19:09|Type : Information|Source : csc_vpnashim|Description : [TID=10348 P

Date : 03/03/2026|Time : 02:19:09|Type : Information|Source : csc_vpnashim|Description : [TID=10348 P

Date : 03/03/2026|Time : 02:19:10|Type : Information|Source : csc_vpnashim|Description : [TID=10348 P

Date : 03/03/2026|Time : 02:19:10|Type : Error|Source : csc_libcsd|Description : Function: open_logfile

Date : 03/03/2026|Time : 02:19:10|Type : Error|Source : csc_libcsd|Description : [Tue Mar 03 02:19:10.3

Date : 03/03/2026|Time : 02:19:10|Type : Error|Source : csc_libcsd|Description : Function: csd_prelogin

Eerste stappen voor probleemoplossing uitgevoerd

Deze stappen voor probleemoplossing zijn geprobeerd:

- De Cisco Secure Client-module opnieuw installeren op de VDI
- De VDI-omgeving opnieuw opstarten

Huidige status en doorlopende resolutie

Er wordt momenteel gewerkt aan een zaak met Cisco Engineering om een geschatte aankomsttijd (ETA) te bepalen voor een oplossing of verbetering met betrekking tot Cisco bug ID CSCwt59834. Updates worden verstrekt als nieuwe informatie beschikbaar komt van het engineeringteam.

verzameling van diagnostische informatie

Voor een juiste diagnose van dit probleem, verzamel deze diagnostische informatie:

- Cisco Secure Client-foutscreenshots met de specifieke foutberichten
- DART-bestanden (Diagnostic and Reporting Tool) van de betreffende VDI-omgeving of het

betreffende systeem.

- Verificatie van de codering van gebruikersnamen, met name voor gebruikers met niet-ASCII-tekens

Observeer deze fouten in de SFP-logboeken onder DART-bundel:

Oorzaak

De hoofdoorzaak van dit probleem is gerelateerd aan defecten in de postuur detectie in de Cisco Secure Client bij het werken binnen Windows 365 VDI-omgevingen of lokale pc's, met name wanneer gebruikersnamen niet-ASCII (2-byte) tekens bevatten. De component voor de postuur-evaluatie kan deze tekencoderingen niet goed verwerken tijdens de fase "hostscan csd-verificatie vooraf", wat leidt tot verbindingfouten.

Dit probleem is gedocumenteerd en bijgehouden onder Cisco bug ID CSCwt59834.

Gerelateerde inhoud

- [Cisco Bug Search - Cisco bug ID CSCwt59834](#)
- [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.