Secure Access Custom CA Trust-problemen met Firefox en Safari op macOS

Inhoud

uitgifte

Gebruikers hebben certificaatvertrouwensfouten ervaren in macOS-browsers (Safari en Firefox) bij het openen van ontsleuteld internetverkeer via Cisco Secure Access. Chrome browser werkte correct, maar Safari en Firefox weergegeven "onvertrouwde certificaat" waarschuwingen en geblokkeerde toegang tot websites en applicaties.

De volledige certificaatketen toonde:

- Website (zoals cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Firefox- en Safari-browsers stopten de certificaatvalidatie bij de Cisco-intermediaire certificaten en slaagden er niet in om een keten tot de root-CA te maken, terwijl Chrome met succes de hele certificaatketen valideerde.

milieu

- Cisco Secure Access-implementatie met aangepaste certificeringsautoriteit voor HTTPS-decodering
- macOS apparaten met Safari en Firefox browsers
- Aangepaste CA-certificaatinfrastructuur met Microsoft Certificate Authority
- Internettoegangsbeleid met decodering en inbraakpreventie ingeschakeld
- Organisatie-ID: xxxxx

resolutie

Het probleem werd opgelost door een coderingsmismatch in de certificaatketen te identificeren en over te schakelen naar de Cisco Secure Access Root CA voor decodering.

analyse van de grondoorzaak

Het team heeft vastgesteld dat de aangepaste certificeringsinstantie is gemaakt met behulp van afdrukbare tekenreekscodering, wat onverenigbaarheidsproblemen veroorzaakte, zelfs wanneer bladcertificaten op UTF8STRING werden ingesteld. Firefox en Safari vereisen dat alle certificaten in een keten in hetzelfde formaat zijn, terwijl Chrome deze strikte vereiste niet heeft.

Afwikkelingsstappen

Switch naar Cisco Secure Access Root CA

Alternatieve oplossingen

Als u een aangepaste CA moet gebruiken, zijn deze opties geïdentificeerd:

- Bouw de volledige certificaatinfrastructuur opnieuw met UTF8-codering (grote impact, niet aanbevolen)
- Gebruik een andere certificaatinfrastructuur die UTF8-codering ondersteunt
- Beperking van Firefox en Safari kan niet werken met de huidige aangepaste CA-instelling

Oorzaak

De hoofdoorzaak was een coderingsmismatch tussen de Microsoft Certificate Authority (die

standaard printable string encoding gebruikt) en de UTF8-keten die wordt gebruikt door Cisco Secure Access. Firefox en Safari hebben strengere certificaatvalidatievereisten en hebben alle certificaten in de keten nodig om consistente codering te gebruiken. de mildere validatie in Chrome liet het werken met de gemengde coderingsketen toe, terwijl Firefox en Safari de inconsistente certificaatformaten verwierpen.

De Microsoft CA heeft certificaten gemaakt met behulp van afdrukbare tekenreekscodering, maar Cisco Secure Access-intermediaire certificaten gebruikten UTF8STRING-codering. Deze mismatch zorgde ervoor dat Firefox en Safari de validatie van de certificaatketen op het Cisco intermediate certificaatniveau mislukten.

Gerelateerde inhoud

- Webex-vergadertoegang configureren in SWG
- 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.