Fout bij verlopen certificaat oplossen tijdens toegang tot paraplu-integratie

Inhoud

Inleiding

In dit document wordt beschreven hoe u een fout bij het verlopen van certificaten kunt oplossen wanneer een Umbrella-integratie toegang krijgt tot s-platform.api.opendns.com of fireeye.vendor.api.opendns.com.

uitgeven

Umbrella-integraties die gebruikmaken van sommige clients van derden, kunnen mislukken met een fout bij het verifiëren van het digitale certificaat van de server voor de Umbrella API's op s-platform.api.opendns.com en fireeye.vendor.api.opendns.com. De fouttekst of -code varieert afhankelijk van het clientprogramma dat in de integratie wordt gebruikt, maar geeft meestal aan dat er een verlopen certificaat aanwezig is.

Oorzaak

Dit probleem wordt niet veroorzaakt door het certificaat van de server, dat momenteel geldig is. Het probleem wordt eerder veroorzaakt door een verouderde certificaatvertrouwenswinkel die door de klant wordt gebruikt.

De webserver die s-platform.api.opendns.com en fireeye.vendor.api.opendns.com bedient maakt gebruik van een digitaal certificaat dat wordt uitgegeven (dat digitaal is ondertekend) door het tussenliggende certificaat R3 van certificaatautoriteit Let's Encrypt. R3 wordt ondertekend door een publieke sleutel die in beide huidige SRG Root X1 root certificaat van Let's Encrypt, en een oudere, cross-signed versie van SRG Root X1. Er bestaan dus twee validatiepaden: één die eindigt bij de huidige SRG Root X1 en één die eindigt bij de uitgever van de gekruiste versie, het DST Root CA X3 certificaat, uitgegeven door certificaatautoriteit IdenTrust.

Een diagram van de uitgifte is beschikbaar bij Let's Encrypt. Bovendien kan de Qualys SSL Labs tool worden gebruikt om de twee "Certificeringspaden" met hun respectievelijke certificaten en de certificaatdetails, zoals de vervaldata, te bekijken.

Root-certificaten worden bewaard in een of meer certificaatvertrouwenswinkels op clientsystemen. Op 30 september 2021 is het DST Root CA X3 certificaat verlopen. Sinds deze datum kunnen clients die het DST Root CA X3-certificaat in hun vertrouwensarchief hebben, maar niet over het nieuwere RG Root X1-hoofdcertificaat beschikken, geen verbinding maken met s-platform.api.opendns.com of fireeye.vendor.api.opendns.com vanwege een certificaatfout. De foutmelding of -code kan een verlopen certificaat als reden voor de fout aangeven. Het verlopen certificaat is het DST Root CA X3-certificaat in het vertrouwensarchief van de client, niet het servercertificaat voor de API-servers s-platform.api.opendns.com en fireeye.vendor.api.opendns.com.

resolutie

Om dit probleem op te lossen, werkt u de vertrouwenswinkel van de client bij met het nieuwe SRG Root X1-certificaat, dat kan worden gedownload van de Let's Encrypt-website. (Deze pagina biedt ook websites voor het testen van uw klanten.) Raadpleeg de documentatie voor uw client of besturingssysteem voor instructies over het bekijken en bijwerken van de vertrouwensopslag van uw client. Als er een officieel updatepakket of automatisch updatemechanisme beschikbaar is, is dit meestal de voorkeur boven het handmatig bijwerken van de vertrouwenswinkel.

Als u het vertrouwensarchief handmatig bijwerkt met het nieuwe SRG Root X1-certificaat, raden we u ook aan het verlopen DST Root CA X3-certificaat te verwijderen, voor het geval dat de validatie van de padcode van uw client problemen oplevert. Een officiële update van de vertrouwenswinkel van de provider van uw client of besturingssysteem kan de SRG Root X1 toevoegen en het DST Root CA X3-certificaat verwijderen.

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.