

SSL-certificaat en handschuiffouten begrijpen in beveiligde toegang

Inhoud

uitgifte

HTTP-verkeer geblokkeerd vanwege certificaat- en TLS-fouten kan nu worden bekeken in de Dashboard Activity Search. Dit artikel bevat een lijst met veelvoorkomende foutmeldingen en een korte uitleg voor elk van de fouten.

milieu

- Cisco Secure Access — Secure Web Gateway SSL Inspection

resolutie

Upstream-certificaat verlopen

Het certificaat van de website is verlopen, dus Cisco Secure Access vertrouwt het niet. Deze is op de website-eigenaar te repareren, dus neem contact op met de webmaster van de site en laat het hen weten.

Upstream Certificaat Zelfondertekend

De website presenteert een certificaat dat het zelf heeft ondertekend, in plaats van een certificaat

dat is uitgegeven door een vertrouwde certificeringsinstantie. Omdat er geen onafhankelijke instantie voor instaat, kan Cisco Secure Access op geen enkele manier bevestigen dat het certificaat echt is.

U ziet vaak zelfondertekende certificaten over bronnen die bedoeld zijn voor een klein, intern publiek - de beheerdersportalen op IT-beveiligingsapparaten zijn een klassiek voorbeeld. Houd er rekening mee dat Cisco Secure Access niet kan worden ingesteld om zelfondertekende certificaten te vertrouwen.

Ontbrekend tussenliggend certificaat

Cisco Secure Access kon niet alle tussentijdse certificaten verzamelen die het nodig heeft, dus het kan de volledige vertrouwensketen niet terugbouwen naar een root.

Hier is waarom dat belangrijk is: een website certificaat (het "blad") wordt ondertekend door een intermediair certificaat, dat op zijn beurt kan worden ondertekend door een andere intermediair, en zo verder tot een vertrouwde wortel. Om deze keten uit te checken, moet de website zijn tussenliggende certificaat (s) samen met zijn eigen verzenden. Als die ontbreken, wordt de validatie onderbroken - dus laat het de webmaster van de site weten.

Er is één uitzondering: als het certificaat de extensie "Authority Information Access" (AIA) bevat, kan Cisco Secure Access proberen de ontbrekende tussenproducten alleen op te halen. Houd er rekening mee dat dit alleen werkt wanneer zowel HTTPS-decodering als bestandsinspectie zijn ingeschakeld.

Upstream-certificaat Ontbrekende onderwerpnaam

Het certificaat bevat geen onderwerpnaam (een Distinguished Name) of een alternatieve onderwerpnaam, wat betekent dat er niets is dat duidelijk aangeeft van wie het certificaat is. Zonder dat kan Cisco Secure Access het niet valideren. Dit is iets wat de website eigenaar moet corrigeren.

Upstream-certificaat ontbreekt algemene naam

Het certificaat heeft geen gemeenschappelijke naam (CN) - het veld dat traditioneel de hostnaam

van de site had en hielp bevestigen dat het certificaat eigenlijk tot de site behoort die u bezoekt. Tegenwoordig hangt die controle echt af van de alternatieve onderwerpnaam (SAN) en wordt CN beschouwd als een legacy-veld, maar de afwezigheid ervan kan deze fout nog steeds veroorzaken. Neem contact op met de webmaster om het te laten behandelen.

Upstream-certificaat niet-vertrouwd

Cisco Secure Access vertrouwt dit certificaat niet, meestal omdat het de root-CA die het heeft uitgegeven niet herkent.

Cisco Secure Access SWG houdt een ingebouwde lijst bij van vertrouwde Root Certificate Authorities, afkomstig van een gerenommeerde provider en up-to-date. Als het certificaat van een site teruggaat naar een CA die niet op die lijst staat, mislukt de validatie. Als u er zeker van bent dat de Root CA een is die u kunt vertrouwen, neem dan contact op met technische ondersteuning en we kunnen een kijkje nemen.

Hostnaam in Cert is anders dan verwacht

Het adres dat u hebt aangevraagd, komt niet overeen met de naam op het certificaat - noch de algemene naam (CN), noch een van de alternatieve onderwerpnamen (SAN). Aangezien het certificaat niet lijkt te behoren tot de site die u bereikt, vertrouwt Cisco Secure Access het niet voor dit verzoek. De webmaster moet dit oplossen.

Upstream-certificaat ingetrokken

De certificeringsinstantie die dit certificaat heeft afgegeven, heeft het inmiddels ingetrokken, met andere woorden, het wordt niet langer als geldig beschouwd.

Cisco Secure Access bevestigt dit met het Online Certificate Status Protocol (OCSP), dat in real time controleert of een certificaat is ingetrokken. Laat het de webmaster van de site weten, zodat ze het kunnen vervangen.

TLS-handschuiffouten

Niet-ondersteunde upstream-codering

De TLS-handshake kon niet worden voltooid omdat de website geen van de coderingssuites ondersteunt die Cisco Secure Access SWG gebruikt. Dit komt meestal voor bij oudere of verouderde servers die alleen zwakkere cijfers bieden. De oplossing is aan de serverzijde, dus geef deze door aan de webmaster.

Upstream TLS-versie komt niet overeen

De handshake is mislukt omdat de website geen TLS-versie gebruikt die Cisco Secure Access SWG ondersteunt. Op dit moment werkt de SWG-proxy van Cisco Secure Access met TLS 1.2 en TLS 1.3 — zowel voor verbindingen die binnenkomen van clients als voor verbindingen die worden gemaakt met bestemmingsservers.

Upstream DH-toets minder dan 1024 bits

De handdruk kon niet worden voltooid omdat de website een Diffie-Hellman-toets gebruikt die te zwak is (minder dan 1024 bits) voor Cisco Secure Access om te accepteren. Dit is een beperking aan de serverzijde, dus de webmaster moet deze versterken.

tijdelijke oplossing

Het is mogelijk om deze problemen op te lossen door configuratiewijzigingen aan te brengen in Cisco Secure Access.

Dit mag alleen als u de authenticiteit van de server en het certificaat vertrouwt.

Workarounds kunnen worden toegepast met behulp van een "Selective Decryption List" -vermelding om decryptie uit te schakelen of een "External Domains" -vermelding om het verkeer van Cisco Secure Access volledig te omzeilen. Cisco Secure Access voert geen certificaatvalidatie uit wanneer decodering is uitgeschakeld.

Houd er rekening mee dat de browser in de meeste gevallen nog steeds een fout of waarschuwing

weergeeft wanneer het verkeer wordt omzeild van Cisco Secure Access - webbrowsers voeren vergelijkbare certificaatvalidatie uit.

Oorzaak

Cisco Secure Access SSL-inspectieproxy kon de TLS-handdruk niet voltooien - meestal omdat de bestemming gebruik maakt van het vastzetten van het certificaat dat het opnieuw ondertekende certificaat van CSA afwijst.

- Pinning van certificaat: harde clientcodes verwachte cert-vingerafdruk
- CSA CA niet vertrouwd op eindpunt: CA-certificaat voor inspectie niet geïmplementeerd in vertrouwde basiswinkel

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.