Common Certificate- en TLS-protocolfouten begrijpen

Inhoud

Inleiding

In dit document worden veelvoorkomende fouten in certificaten en TLS-protocollen beschreven in de zoekfunctie voor activiteiten in het overkoepelende dashboard.

Overzicht

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

Certificaatfouten

Upstream-certificaat verlopen

Een certificaat dat door de website wordt gepresenteerd, is verlopen. Neem contact op met de webmaster van de site om dit probleem te melden.

Upstream-certificaat zelf ondertekend

Het servercertificaat dat door de website wordt gepresenteerd, is niet ondertekend door een certificeringsinstantie en daarom kan Umbrella niet bepalen of het certificaat betrouwbaar is.

Zelfondertekende certificaten worden soms gebruikt wanneer een server een bron host die bedoeld is voor een beperkt publiek. Webportals voor IT-beveiligingstoestellen gebruiken bijvoorbeeld vaak zelf ondertekende certificaten. De paraplu kan niet worden geconfigureerd om zelfondertekende certificaten te vertrouwen.

ontbrekend tussentijds certificaat

Umbrella was niet in staat om certificaten voor alle bemiddelende instanties te verkrijgen en kon daarom de volledige vertrouwensketen niet valideren.

Webservercertificaten worden doorgaans uitgegeven/ondertekend door een tussenliggend certificaat van een certificeringsinstantie. Deze tussentijdse certificaten kunnen ook worden afgegeven door andere tussentijdse certificaten. Het webservercertificaat (ook bekend als "leaf certificaat") en eventuele tussenliggende certificaten vormen een keten terug naar een root-certificaat. De website moet de tussenliggende certificaten bundelen met het servercertificaat zodat Umbrella de volledige vertrouwensketen kan valideren. Neem contact op met de webmaster van de site om dit probleem te melden.

Als het certificaat ook de extensie "Toegang tot informatie van de autoriteit" bevat, probeert Umbrella de CA's voor tussenpersonen automatisch op te halen. Umbrella ondersteunt de AIA-extensie alleen wanneer HTTPS-decodering en bestandsinspectie zijn ingeschakeld.

Upstream certificaat ontbrekende onderwerpnaam.

Het veld Onderwerp van het certificaat bevat geen DN (Distinguished Name) om dit certificaat te identificeren. Dit is een vereiste voor alle certificaten die zijn uitgegeven door een certificeringsinstantie en daarom vereist door Cisco Umbrella. Neem contact op met de webmaster van de site om dit probleem te melden.

Upstream-certificaat ontbreekt algemene naam.

Het certificaat dat door de website wordt gepresenteerd, heeft geen gemeenschappelijke naam. Het veld Gemeenschappelijke naam (GN) is vereist door Umbrella SWG. Dit bevat de hostnaam van het certificaat, die vereist is om te valideren dat het certificaat overeenkomt met de bron die door de gebruiker is aangevraagd (bijv. Het adres wordt in de browser ingevoerd). Neem contact op met de webmaster van de site om dit probleem te melden.

Upstream-certificaat niet vertrouwd

Het certificaat wordt niet vertrouwd door Cisco Umbrella. Deze fout betekent meestal dat Cisco de basiscertificeringsinstantie die het certificaat heeft afgegeven, niet vertrouwt.

Umbrella SWG heeft een ingebouwde lijst met bekende vertrouwde Root Certificate Authorities die we bijwerken vanuit een gerenommeerde bron. Als het certificaat van de website niet is

ondertekend door een CA in deze lijst, mislukt de validatie van het certificaat. Als u denkt dat Umbrella een Root CA mist die betrouwbaar is, neem dan contact op met de technische ondersteuning.

Hostnaam in cert is anders dan verwacht

De door de gebruiker gevraagde bron (bijv. het adres dat in de browser is ingevoerd) komt niet overeen met de algemene naam (CN) of alternatieve onderwerpnaam (SAN) van het certificaat, dus Umbrella kan het certificaat voor dit verzoek niet vertrouwen. Neem contact op met de webmaster van de site om dit probleem te melden.

Upstream-certificaat ingetrokken

Het door de website verstrekte certificaat is ingetrokken door de instantie die het certificaat heeft afgegeven.

Umbrella voert OCSP (Online Certificate Status Protocol)-controles uit om te bepalen of een certificaat later is ingetrokken door een CA. Neem contact op met de webmaster van de site om dit probleem te melden.

TLS-handshake-fouten

Niet-ondersteunde upstreamversleuteling

De TLS-handdruk kon niet worden voltooid. Dit betekent meestal dat de website geen enkele van de lijst met Cypher Suites ondersteunt die door Umbrella SWG wordt gebruikt. Deze fout kan optreden bij oudere of verouderde webservers die alleen zwakkere TLS-coderingen ondersteunen. Neem contact op met de webmaster van de site om dit probleem te melden.

Mismatch upstream TLS-versie

De TLS-handdruk kon niet worden voltooid omdat de website niet dezelfde TLS-versie ondersteunt die Umbrella SWG gebruikt. Op dit moment ondersteunt Umbrella SWG Proxy TLS 1.2 en TLS 1.3 op zowel de verbindingen aan de clientzijde met Umbrella SWG als van Umbrella SWG-proxyverbindingen met bestemmingswebservers.

Upstream DH-sleutel minder dan 1024 bits

De TLS-handdruk kon niet worden voltooid omdat de website een zwakke Diffie-Hellman-sleutel gebruikt die niet wordt ondersteund door Umbrella. Neem contact op met de webmaster van de site om dit probleem te melden.

tijdelijke oplossingen

Het is mogelijk om deze problemen op te lossen door configuratiewijzigingen aan te brengen in Cisco Umbrella. Dit moet alleen worden gedaan als u de authenticiteit van de server en het

certificaat vertrouwt.

Workarounds kunnen worden toegepast met behulp van een "Selective Decryption List" -item om decodering uit te schakelen of een "Externe domeinen" -item om het verkeer van Umbrella volledig te omzeilen. Umbrella voert geen certificaatvalidatie uit wanneer decodering is uitgeschakeld. Houd er rekening mee dat in de meeste gevallen de browser nog steeds een fout of waarschuwing geeft wanneer het verkeer wordt omzeild van Umbrella - webbrowsers voeren vergelijkbare certificaatvalidatie uit.

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.