

Probleemoplossingsfout " 517 Upstream-certificaat ingetrokken"

Inhoud

[Inleiding](#)

[uitgeven](#)

[Oorzaak](#)

[Verskillend gedrag bij direct browsen](#)

[resolutie](#)

[Aanvullende informatie](#)

Inleiding

In dit document wordt beschreven hoe u de fout "517 Upstream Certificate Revoked" kunt oplossen wanneer u naar een HTTPS-URL bladert.

uitgeven

Wanneer de webproxy Umbrella Secure Web Gateway (SWG) is geconfigureerd om HTTPS-inspectie uit te voeren, kan een gebruiker een 517 Upstream Certificate Revoked-foutpagina ontvangen. Deze fout geeft aan dat de gevraagde website een digitaal certificaat heeft verzonden in de TLS-onderhandeling dat volgens de uitgever van dat certificaat of een vergelijkbare autoriteit de status "ingetrokken" heeft. Een ingetrokken certificaat is niet meer geldig.



517 Upstream Certificate Revoked

The SSL security certificate presented by this site has been revoked by the certificate authority. This means attackers might be trying to steal your information (for example, passwords, messages, or credit cards). If you continue seeing this error, please contact your Administrator.

This page is served by Umbrella Cloud Security Gateway. Server: mps-1556a1994fc3.sigenvl.sin

Fri, 15 Jan 2021 12:27:39 GMT

13351060307092

Oorzaak

Wanneer een Umbrella-client een HTTPS-verzoek doet via de Umbrella Secure Web Gateway, voert SWG certificaatintrekkingscontroles uit met behulp van het [Online Certificate Status Protocol \(OCSP\)](#). OCSP geeft de intrekkingstatus van een certificaat aan. SWG doet namens de Umbrella-klanten OCSP-aanvragen voor de status van certificaatintrekking.

SWG bepaalt de status voor het intrekken van certificaten van de aangevraagde webserver en alle tussenliggende certificaten die worden uitgegeven in het pad naar een vertrouwd rootcertificaat. Deze controles zorgen ervoor dat een geldige keten van vertrouwen niet ongeldig is geworden sinds de uitgifte.

In een digitaal certificaat dat OCSP-intrekkingscontrole gebruikt, bevat de extensie "Authority Information Access" X.509 een of meer "OCSP"-velden. Een veld bevat een HTTP-URL voor een OCSP-eindpunt (webserver) dat kan worden opgevraagd voor de intrekkingstatus van het certificaat. SWG doet verzoeken naar elke OCSP-URL in een certificaat totdat een antwoord is ontvangen dat een van de volgende opties aangeeft:

- het certificaat is geldig (niet ingetrokken) op het moment dat SWG het webverzoek toestaat om door te gaan, OF
- iets anders dan een OCSP "certificaat geldig" antwoord (bijvoorbeeld het certificaat wordt ingetrokken, de server kan op dit moment niet antwoorden, een HTTP-foutstatus, een time-out van een netwerk/transportlaag, enzovoort) op welk moment SWG de juiste foutpagina/bericht presenteert en het webverzoek mislukt

Merk op dat OCSP-antwoorden meestal in de cache worden opgeslagen en worden gebruikt om te reageren op toekomstige controles. De cachetijd wordt ingesteld door de server in de OCSP-respons.

Verschillend gedrag bij direct browsen

Webclients kunnen verschillende controlemechanismen voor herroeping gebruiken, afhankelijk van de client. De Chrome-browser van Google maakt bijvoorbeeld standaard geen gebruik van de OCSP- of de standaard CRL-methoden. In plaats daarvan gebruikt Chrome een eigen versie van een CRL genaamd [CRLSet](#), die Secure Web Gateway niet gebruikt. Als gevolg hiervan kan Chrome niet hetzelfde resultaat als SWG produceren bij het controleren van de intrekingsstatus van een certificaat.

Merk echter op dat, zoals de CRLSet-documentatie aangeeft, "in sommige gevallen de onderliggende systeemcertificaatbibliotheek deze controles altijd uitvoert, ongeacht wat Chromium doet." Afhankelijk van uw lokale omgeving kan een OCSP- en/of CRL-controle dus worden uitgevoerd door uw browser of de cryptografische servicebibliotheek van het besturingssysteem, zoals SChannel, Secure Transport of NSS.

Merk ook op dat OCSP- en CRL-controles niet gegarandeerd hetzelfde resultaat opleveren.

Raadpleeg de documentatie van de leverancier van uw browser of besturingssysteem om te bepalen welke certificaatintrekkingscontroles door uw klanten worden uitgevoerd tijdens het browsen.

resolutie

Het gebruik van geldige certificaten is de verantwoordelijkheid van de webserverbeheerder. Herstel van ingetrokken certificaten moet door de serverbeheerder op de server worden uitgevoerd. Cisco Umbrella kan niet helpen bij dit proces.

Cisco Umbrella raadt u ten eerste af om toegang te krijgen tot een website die een ingetrokken certificaat gebruikt. Work-arounds kunnen alleen worden gebruikt als de gebruiker volledig begrijpt waarom een site een ingetrokken certificaat gebruikt en alle risico's volledig accepteert.

Om de fout te voorkomen, kan de site worden vrijgesteld van HTTPS-inspectie door een selectieve decoderingslijst te maken met de domeinnaam van de site. De selectieve decoderingslijst wordt toegepast op het webbeleid dat toegang tot de site mogelijk maakt. Als alternatief kan de site worden toegevoegd aan de lijst Externe domeinen om verkeer rechtstreeks naar de site te sturen, waarbij SWG wordt omzeild.

Aanvullende informatie

Klanten die willen bevestigen of het certificaat van een server is ingetrokken, kunnen gebruikmaken van tools van derden die zijn ontworpen om de intrekingsstatus te controleren. Met name de SSL Server Test tool van Qualys SSL Labs voert zowel OCSP- als CRL-controles uit, naast het verstrekken van andere informatie over de geldigheid van certificaten. De tool is online

beschikbaar op:

- <https://www.ssllabs.com/ssltest/analyze.html>

We raden u aan deze tool te gebruiken om de site te controleren die een fout met een 517 Upstream Certificate Revoked-fout produceert, voordat u een supportcase opent met Cisco Umbrella.

Zie ook: <https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors>

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.