Fehlerbehebung Fehler "517 Upstream-Zertifikat widerrufen"

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für den Fehler "517 Upstream Certificate Revoked" beim Navigieren zu einer HTTPS-URL beschrieben.

Problem

Wenn der Umbrella Secure Web Gateway (SWG)-Webproxy für die HTTPS-Inspektion konfiguriert ist, kann ein Benutzer eine Fehlerseite 517 Upstream Certificate Revoked empfangen. Dieser Fehler zeigt an, dass die angeforderte Website ein digitales Zertifikat in der TLS-Verhandlung gesendet hat, das den Status "widerrufen" hat, je nachdem, ob das Zertifikat ausgestellt wurde oder eine ähnliche Behörde. Ein gesperrtes Zertifikat ist nicht mehr gültig.

13351060307092

Ursache

Wenn ein Umbrella-Client eine HTTPS-Anfrage über das Umbrella Secure Web Gateway stellt, führt die SWG mithilfe des Online Certificate Status Protocol (OCSP) Prüfungen zum Widerruf von Zertifikaten durch. Der OCSP stellt den Sperrstatus eines Zertifikats bereit. Die SWG stellt im Namen der Umbrella-Clients OCSP-Anfragen zum Widerruf des Zertifikats.

SWG bestimmt den Status des Zertifikatswiderrufs des angeforderten Webserver-Zertifikats und alle ausstellenden Zwischenzertifikate im Pfad zu einem vertrauenswürdigen Stammzertifikat. Diese Prüfungen stellen sicher, dass eine gültige Vertrauenskette seit der Ausstellung nicht ungültig geworden ist.

In einem digitalen Zertifikat, das die OCSP-Widerrufsprüfung verwendet, enthält die X.509-Erweiterung "Authority Information Access" ein oder mehrere "OCSP"-Felder. Ein Feld enthält eine HTTP-URL für einen OCSP-"Endpunkt" (Webserver), der nach dem Sperrstatus des Zertifikats abgefragt werden kann. Die SWG fordert alle OCSP-URLs in einem Zertifikat an, bis eine Antwort eingeht, die einen der folgenden Hinweise gibt:

- das Zertifikat gültig ist (nicht widerrufen), wenn die SWG die Fortsetzung der Webanfrage gestattet, ODER
- etwas Anderes als eine OCSP "certificate valid"-Antwort (z. B. das Zertifikat wird widerrufen, der Server kann derzeit keine Antwort geben, ein HTTP-Fehlerstatus, eine Netzwerk-/Transportschicht-Zeitüberschreitung usw.), wenn die SWG die entsprechende Fehlerseite/Fehlermeldung anzeigt und die Webanfrage fehlschlägt

Beachten Sie, dass OCSP-Antworten in der Regel zwischengespeichert und für zukünftige Prüfungen verwendet werden. Die Caching-Zeit wird vom Server in der OCSP-Antwort festgelegt.

Unterschiedliches Verhalten beim direkten Surfen

Webclients können je nach Client verschiedene Mechanismen zur Sperrungsprüfung verwenden. Beispielsweise verwendet der Google-Browser Chrome standardmäßig weder die OCSP- noch die Standard-CRL-Methode. Stattdessen verwendet Chrome eine proprietäre Version einer CRL mit dem Namen CRLSet, die Secure Web Gateway nicht verwendet. Infolgedessen kann Chrome beim Überprüfen des Widerrufsstatus eines Zertifikats möglicherweise nicht das gleiche Ergebnis wie SWG liefern.

Beachten Sie jedoch, dass, wie in der CRLSet-Dokumentation festgestellt wird, "in einigen Fällen die zugrunde liegende Systemzertifikatbibliothek diese Prüfungen immer durchführt, unabhängig davon, was Chrom tut." Je nach Ihrer lokalen Umgebung kann eine OCSP- und/oder CRL-Prüfung entweder von Ihrem Browser oder von den kryptografischen Service-Bibliotheken des Betriebssystems, wie SChannel, Secure Transport oder NSS, durchgeführt werden.

Beachten Sie auch, dass OCSP- und CRL-Prüfungen nicht garantiert das gleiche Ergebnis liefern.

Lesen Sie in der Dokumentation Ihres Browsers oder des Betriebssystemanbieters nach, um herauszufinden, welche Prüfungen zum Widerruf von Zertifikaten von Ihren Clients beim Surfen durchgeführt werden.

Auflösung

Die Verwendung von gültigen Zertifikaten liegt in der Verantwortung des Webserver-Administrators. Die Bereinigung der gesperrten Zertifikate muss vom Serveradministrator auf dem Server durchgeführt werden. Cisco Umbrella kann diesen Prozess nicht unterstützen.

Cisco Umbrella rät dringend davon ab, auf eine Website zuzugreifen, die ein widerrufenes Zertifikat verwendet. Workarounds können nur angewendet werden, wenn der Benutzer die Gründe für die Verwendung eines widerrufenen Zertifikats durch eine Website vollständig versteht und alle Risiken eingeht.

Um den Fehler zu vermeiden, kann die Site von der HTTPS-Überprüfung ausgenommen werden, indem eine Liste selektiver Entschlüsselung erstellt wird, die den Domänennamen der Site enthält. Die selektive Entschlüsselungsliste wird auf die Webrichtlinie angewendet, die den Zugriff auf die Website zulässt. Alternativ kann der Standort der Liste Externe Domänen hinzugefügt werden, um Datenverkehr unter Umgehung der SWG direkt an den Standort zu senden.

Zusätzliche Informationen

Kunden, die bestätigen möchten, ob das Serverzertifikat widerrufen wurde, können Tools von Drittanbietern verwenden, um den Widerrufsstatus zu überprüfen. Insbesondere führt das SSL-Servertest-Tool von Qualys SSL Labs OCSP- und CRL-Prüfungen durch und stellt weitere Informationen zur Gültigkeit von Zertifikaten bereit. Das Tool ist online verfügbar unter:

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

Wir empfehlen, dieses Tool zu verwenden, um die Site zu überprüfen, die einen Fehler "517 Upstream Certificate Revoked" verursacht, bevor Sie ein Support-Ticket bei Cisco Umbrella erstellen.

Siehe auch: https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.