Fehlerbehebung beim Zertifikatablauffehler beim Zugriff auf Umbrella Integration

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Fehler beim Ablauf eines Zertifikats beheben, wenn eine Umbrella-Integration auf s-platform.api.opendns.com oder fireeye.vendor.api.opendns.com zugreift.

Problem

Umbrella-Integrationen, die einige Drittanbieter-Clients verwenden, können mit einem Fehler scheitern, der das digitale Zertifikat des Servers für die Umbrella-APIs verifiziert: s-platform.api.opendns.com and fireeye.vendor.api.opendns.com. Der Fehlertext oder -code variiert je nach dem bei der Integration verwendeten Clientprogramm, weist jedoch in der Regel darauf hin, dass ein abgelaufenes Zertifikat vorhanden ist.

Ursache

Dieses Problem wird nicht durch das derzeit gültige Serverzertifikat verursacht. Stattdessen wird das Problem durch einen veralteten Zertifikatvertrauensspeicher verursacht, der vom Client verwendet wird.

Der Webserver, der s-platform.api.opendns.com und fireeye.vendor.api.opendns.com bedient, verwendet ein digitales Zertifikat, das vom Zwischenzertifikat R3 der Zertifizierungsstelle Let's Encrypt ausgestellt (digital signiert) wird. R3 wird von einem öffentlichen Schlüssel signiert, der in beiden aktuellen SRG Root X1 Root-Zertifikat von Let's Encrypt und eine ältere, kreuzsignierte Version von SRG Root X1. Es existieren also zwei Validierungspfade: eines, das am aktuellen SRG-Root X1 endet, und eines, das am Aussteller der signaturübergreifenden Version, dem von der Zertifizierungsstelle IdenTrust ausgestellten DST-Root-CA X3-Zertifikat, endet.

Ein Diagramm der Ausgabe finden Sie unter Let's Encrypt. Darüber hinaus können mit dem Qualys SSL Labs-Tool die beiden "Zertifizierungspfade" mit den jeweiligen Zertifikaten und die Zertifikatdetails, z. B. das Ablaufdatum, angezeigt werden.

Stammzertifikate werden in einem oder mehreren Zertifikatvertrauensspeichern auf Clientsystemen aufbewahrt. Am 30. September 2021 lief das Zertifikat der DST Root CA X3 aus. Seit diesem Datum stellen Clients, die das Zertifikat DST Root CA X3 in ihrem Trust Store haben, aber nicht über das neuere RG Root X1 Root-Zertifikat verfügen, aufgrund eines Zertifikatfehlers keine Verbindung zu s-platform.api.opendns.com oder fireeye.vendor.api.opendns.com her. Die Fehlermeldung oder der Fehlercode kann ein abgelaufenes Zertifikat als Grund für den Fehler angeben. Das abgelaufene Zertifikat ist das DST Root CA X3-Zertifikat im Trust Store des Clients, nicht das Serverzertifikat für die API-Server s-platform.api.opendns.com und fireeye.vendor.api.opendns.com.

Auflösung

Um dieses Problem zu beheben, aktualisieren Sie den Trust Store des Clients, sodass er das neue SRG Root X1-Zertifikat enthält, das von der Let's Encrypt-Website heruntergeladen werden kann. (Auf dieser Seite finden Sie auch Websites zum Testen Ihrer Clients.) In der Dokumentation für den Client oder das Betriebssystem finden Sie Anweisungen zum Anzeigen und Aktualisieren des Vertrauensspeichers des Clients. Wenn ein offizielles Aktualisierungspaket oder ein automatischer Aktualisierungsmechanismus verfügbar ist, ist dies in der Regel besser als eine manuelle Aktualisierung des Vertrauensspeichers.

Wenn Sie den Trust Store manuell mit dem neuen SRG Root X1-Zertifikat aktualisieren, empfehlen wir, das abgelaufene DST Root CA X3-Zertifikat zu entfernen, falls der Validierungspfaderstellungscode Ihres Clients problematisch ist. Ein offizielles Update des Trust Stores vom Anbieter Ihres Clients oder Betriebssystems kann den SRG Root X1 hinzufügen und das Zertifikat der DST Root CA X3 entfernen.

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.