Sicherer Zugriff Benutzerdefinierte CA Trust Probleme mit Firefox und Safari auf macOS

Inhalt

Problem

Beim Zugriff auf entschlüsselten Internetverkehr über Cisco Secure Access traten in macOS-Browsern (Safari und Firefox) Zertifikatvertrauensfehler auf. Chrome-Browser funktionierte korrekt, aber Safari und Firefox angezeigt "nicht vertrauenswürdige Zertifikate" Warnungen und blockiert den Zugriff auf Websites und Anwendungen.

Die gesamte Zertifikatskette zeigte Folgendes:

- Website (z. B. cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Firefox und Safari-Browser stoppten die Zertifikatsvalidierung bei den Zwischenzertifikaten von Cisco und versäumten es, bis zur Root-Zertifizierungsstelle zu ketten, während Chrome erfolgreich die gesamte Zertifikatskette validierte.

Umwelt

- Cisco Secure Access-Bereitstellung mit benutzerdefinierter Zertifizierungsstelle für HTTPS-Entschlüsselung
- macOS Geräte mit Safari und Firefox Browsern
- Benutzerdefinierte Zertifizierungsstellen-Zertifikatinfrastruktur mit Microsoft Certificate Authority
- Richtlinien für den Internetzugriff mit aktivierter Entschlüsselung und Intrusion Prevention
- Organisations-ID: xxxxx

Auflösung

Das Problem wurde behoben, indem eine Codierungsungleichheit in der Zertifikatskette festgestellt und zur Entschlüsselung zur Cisco Secure Access-Stammzertifizierungsstelle gewechselt wurde.

Ursachenanalyse

Das Team erkannte, dass die benutzerdefinierte Zertifizierungsstelle mit einer druckbaren Zeichenfolgencodierung erstellt wurde, was zu Inkompatibilitätsproblemen führte, selbst wenn Blattzertifikate auf UTF8STRING festgelegt wurden. Firefox und Safari erfordern, dass alle Zertifikate in einer Kette im gleichen Format sein, während Chrome nicht über diese strenge Anforderung.

Lösungsschritte

Wechsel zur Cisco Secure Access Root-CA

Alternative Lösungen

Wenn die Verwendung einer benutzerdefinierten Zertifizierungsstelle erforderlich ist, wurden folgende Optionen festgelegt:

- Erstellen Sie die gesamte Zertifikatsinfrastruktur mit UTF8-Codierung neu (hohe Auswirkung, nicht empfohlen).
- Verwendung einer anderen Zertifikatsinfrastruktur, die UTF8-Codierung unterstützt
- Einschränkung von Firefox und Safari kann nicht mit der aktuellen benutzerdefinierten CA-Konfiguration funktionieren

Ursache

Die Ursache hierfür war ein Codierungsgefälle zwischen der Microsoft Certificate Authority (die standardmäßig die printable Zeichenfolgencodierung verwendet) und der von Cisco Secure Access verwendeten UTF8-Kette. Firefox und Safari haben strengere Anforderungen an die Zertifikatsvalidierung und benötigen alle Zertifikate in der Kette, um eine konsistente Kodierung zu verwenden. die mildere Validierung in Chrome erlaubt es, mit der gemischten Kodierungskette zu arbeiten, während Firefox und Safari die inkonsistenten Zertifikatformate abgelehnt.

Die Microsoft-Zertifizierungsstelle hat Zertifikate mit druckbarer Zeichenfolgencodierung erstellt, die Zwischenzertifikate von Cisco Secure Access verwenden jedoch UTF8STRING-Codierung. Diese Diskrepanz führte dazu, dass Firefox und Safari die Zertifikatkette auf der Cisco Zwischenzertifikatsebene nicht validierten.

Verwandte Inhalte

- Konfigurieren des WebEx Meeting-Zugriffs in SWG
- Technischer Support und Downloads von Cisco

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.