Konfigurieren des Charles-Proxys zum Erfassen von HTTPS-Datenverkehr mit Mac

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Zugehörige Informationen

Einführung

In diesem Dokument wird das Verfahren beschrieben, mit dem HTTPS (Hyper Text Transfer Protocol Secure)-Datenverkehr mit dem Charles-Proxy des Macintosh(Mac)-Programms erfasst wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit Apple OS X vertraut sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Anwendung Charles, die aus der Quelle des Autors verfügbar ist.

Die Informationen in diesem Dokument basieren auf Apple OS X.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Dies ist für die Behebung von SSO-Datenverkehr (Single Sign-On) unerlässlich, der nicht mit normalen Tools für den Netzwerkverkehr erfasst werden kann.

Konfigurieren

Schritt 1: Laden Sie den Charles-Proxy herunter, und installieren Sie dann Charles -Herunterladen der Charles Web Debugging-Proxy-Anwendung

Schritt 2: Open Charles

Schritt 3: Navigieren Sie zu **Proxy** > wählen Sie **MAC OS X Proxy aus.**

Schritt 4: Navigieren Sie zu **Proxy > Proxy Settings >** Enable **Use a dynamic port**

Schritt 5: Navigieren Sie zu Hilfe > SSL Proxying > Install Charles Root Certificate.

Schritt 6: TDas Charles-Proxy-Zertifikat wird unter der **Anmeldung** installiert, jedoch in den **System-**Keystore verschoben.

Keychains login Local Items System System Roots	Certificate (built on Z Root certificate authority Expires: Monday, May 29, 2045 at 11:31:37 China Standard T This certificate is marked as trusted for this account	HIG
	Name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	- Kin pub priv
Category	AirPlay Client Identity: 87bd7d04 AirPlay Client Peer: ae8a2dd4 AirPlay Client Peer: fb6680a9	AirF AirF AirF
Passwords Secure Notes My Contification	 Apple Persistent State Encryption blizzard Charles Proxy Custom Root Ceruilt on ZHIGAO-M-F199, 1 Apr 2016) 	app 802 cert
 Keys Certificates 	com.apple.scopedbookmarksagent.xpc com.cisco.jabber.WebEx DigiCert Assured ID Root CA	app app cert

Schritt 7: Geben Sie Website-URL im Browser und dann Charles erfasst die Protokolle mit den Website-Informationen.

	Charles 3.11.4	4 - Session 1 *
🔄 📫 🛍 🗑 🖊 🢽	1 🕘 🎢 🧃	S / 🖌 💥 🏶
Structure Sequence	(Overview Summary Chart
▼ A https://cisco.webex.com	Name	Value
<pre></pre>	Host	https://cisco.webex.com
	Path	/
	Notes	SSL Proxying not enabled for this host. Enable in the Prox
	w Requests	4
	Completed	4

Schritt 8: Klicken Sie mit der rechten Maustaste auf die Website-URL <u>http://cisco.webex.com</u>, und wählen Sie **SSL-Proxy aktivieren aus.**

Schritt 9: Wählen Sie **Proxy** > **SSL Proxying Settings** > Verify you see this image

Charles	can show you the plain text contents of SSL requests and responses. Only
the loca certifica	tions listed below will be proxied. Charles will issue and sign SSL tes, please press the Help button for more information.
🗹 Enat	ble SSL Proxying
_ Locatio	ns
	cisco.webex.com:443

Charles wird jetzt anfangen den HTTPS-Datenverkehr für die Site-URL erfassen. Um eine andere Site-URL zu erfassen, wiederholen Sie die Schritte 7, 8 und 9, und stellen Sie sicher, dass die URL zur SSL-Proxy-Funktion hinzugefügt wird.

Zugehörige Informationen

<u>Charles Proxy</u>