Beheben Sie Umbrella Root Certificate Fehler bei der Verwendung von Chrome unter Windows

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Umbrella Root-Zertifikatfehler für *cisco.com behoben werden können, wenn Chrome unter Windows verwendet wird.

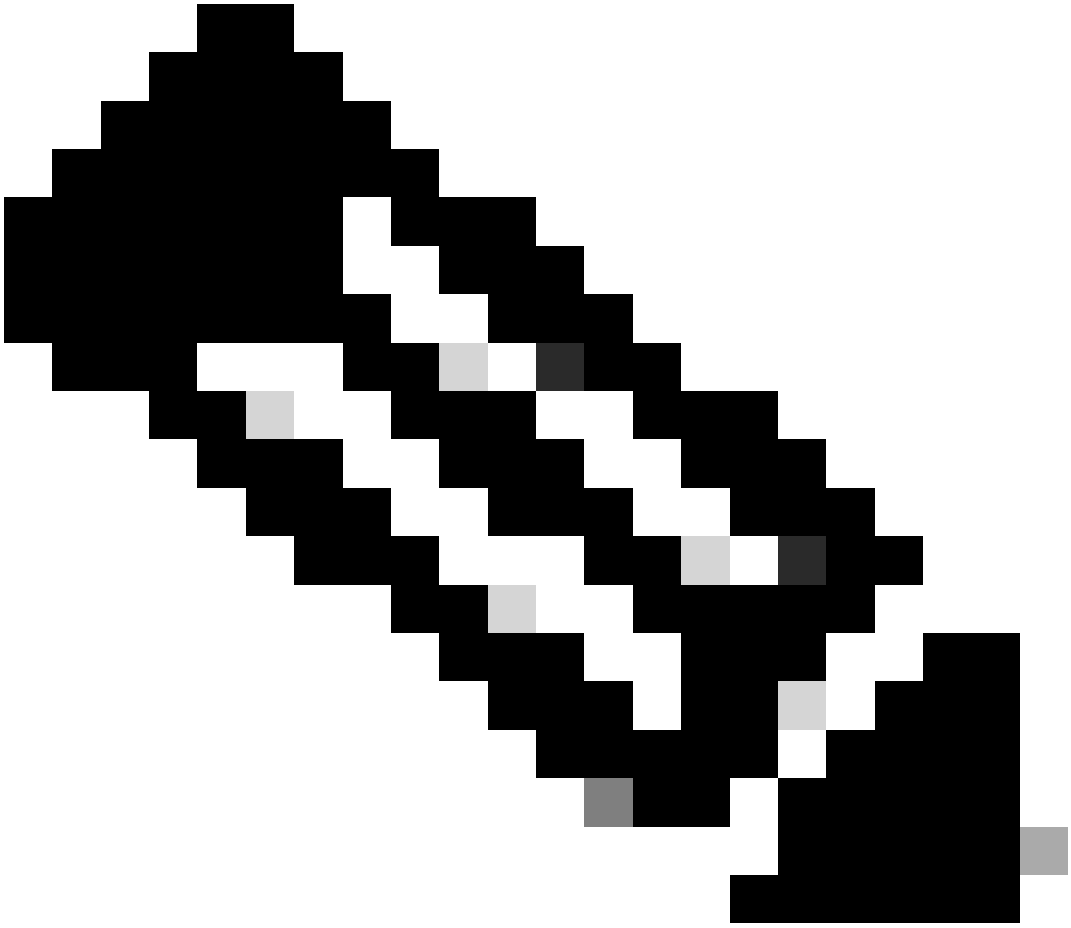
Überblick

Wir haben jetzt eine besser verwaltbare und dauerhafte Lösung für dieses Problem, das für alle Standorte gilt. Obwohl die hier bereitgestellten Informationen weiterhin relevant sind, empfehlen wir, die dauerhafte Lösung durch die Installation der Cisco Root CA zu erkunden, wie in diesem Artikel beschrieben:

https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information

Diese Seite ist eine Anleitung, wenn ein Zertifikatfehler für *.cisco.com in Chrome (für Windows) angezeigt wird, sie kann jedoch nicht umgangen werden, indem eine Zertifikatausnahme hinzugefügt wird.

Die Ursache für diese Meldung ist die Implementierung von HTTP Strict Transport Security (HSTS) oder vorinstallierter Certificate Pinning in modernen Browsern, die ihre allgemeine Sicherheit verbessert. Diese zusätzliche Sicherheit für HTTPS-Seiten verhindert, dass die Umbrella-Blockseite und der Umgehungs-Blockseitenmechanismus funktionieren, wenn HSTS für eine Website aktiv ist. Weitere Informationen zu HSTS finden Sie in diesem Artikel.



Anmerkung: Aufgrund von Änderungen im HSTS funktioniert das BPB-System (Block Page Bypass) aufgrund nicht umgehbarer Zertifikatfehler nicht mit bestimmten Standorten. Damit diese Websites mit BPB in Chrome (für Windows) arbeiten können, müssen Sie beim Starten des Browsers einen speziellen Schalter verwenden. Einige gängige Websites, die nicht mit BPBin Chrome funktionieren, sind: Facebook, Google Sites wie Gmail und YouTube, Dropbox und Twitter. Eine vollständige Liste der Websites finden Sie hier.

Ohne Chrome Certificate Checks zu deaktivieren, scheitern Versuche, die Blockseitenumgehung mit einer der Websites auf dieser geschützten Liste zu verwenden, wie dargestellt.

Deaktivieren von Chrome-Zertifikatprüfungen (nur Windows)

Um Chrome zu zwingen, diese Fehler zu ignorieren, müssen Sie Ihre Verknüpfung für Chrome,

um die Anwendung mit diesem Schalter zu starten:

```
--ignore-certificate-errors
```

Beachten Sie, dass Google diese Funktion jederzeit entfernen kann und daher nur empfohlen wird, solange sie verfügbar ist:

Um dieses Kommandozeilen-Flag zu Chrome hinzuzufügen, klicken Sie mit der rechten Maustaste auf das Chrome-Symbol, wählen Sie "Eigenschaften" und fügen Sie es zu dem und wählen Sie "Eigenschaften", dann fügen Sie es zu dem Ziel wie hier gezeigt:

Sobald dieses Flag hinzugefügt wurde, können Sie BPB normal an den Standorten in der vorinstallierten HSTS-Liste verwenden, um diese zu umgehen.

Obwohl sich in diesem Beispiel twitter.com in der Liste der vorinstallierten HSTS-Zertifikate befindet, können Sie, wenn Sie die Zertifikatswarnung ignorieren, die Funktion "Blockieren von Seitenumgehungen" verwenden.

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.