Accès sécurisé Problèmes de confiance CA personnalisée avec Firefox et Safari sur macOS

Table des matières

Problème

Les utilisateurs ont rencontré des erreurs de confiance de certificat dans les navigateurs macOS (Safari et Firefox) lors de l'accès au trafic Internet décrypté via Cisco Secure Access. Le navigateur Chrome fonctionne correctement, mais Safari et Firefox affichent des avertissements de « certificat non approuvé » et bloquent l'accès aux sites Web et aux applications.

La chaîne de certificats complète montrait :

- Site Web (tel que cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Les navigateurs Firefox et Safari ont arrêté la validation des certificats au niveau des certificats intermédiaires Cisco et n'ont pas réussi à établir une chaîne jusqu'à l'autorité de certification racine, tandis que Chrome a validé avec succès l'ensemble de la chaîne de certificats.

Environnement

- Déploiement de Cisco Secure Access avec autorité de certification personnalisée pour le déchiffrement HTTPS
- appareils macOS avec navigateurs Safari et Firefox
- Infrastructure de certificat CA personnalisée utilisant l'autorité de certification Microsoft
- Politiques d'accès à Internet avec déchiffrement et prévention des intrusions activés
- ID d'organisation : xxxxx

Résolution

Le problème a été résolu en identifiant une non-correspondance de codage dans la chaîne de certificats et en basculant vers l'autorité de certification racine d'accès sécurisé Cisco pour le déchiffrement.

Analyse de la cause première

L'équipe a identifié que l'autorité de certification personnalisée a été créée à l'aide du codage de chaîne imprimable, ce qui a causé des problèmes d'incompatibilité même lorsque les certificats leaf étaient définis sur UTF8STRING. Firefox et Safari exigent que tous les certificats d'une chaîne soient dans le même format, tandis que Chrome n'a pas cette exigence stricte.

Étapes de résolution

Basculer vers l'autorité de certification racine Cisco Secure Access

Solutions alternatives

Si vous devez utiliser une autorité de certification personnalisée, les options suivantes ont été identifiées :

- Reconstruire l'infrastructure de certificat entière à l'aide du codage UTF8 (impact élevé, non recommandé)
- Utiliser une autre infrastructure de certificat qui prend en charge le codage UTF8
- La limitation de Firefox et Safari ne peut pas fonctionner avec la configuration personnalisée actuelle de l'AC

Motif

La cause principale était une non-correspondance de codage entre l'autorité de certification Microsoft (qui utilise le codage printablestring par défaut) et la chaîne UTF8 utilisée par Cisco Secure Access. Firefox et Safari ont des exigences de validation de certificat plus strictes et ont besoin de tous les certificats de la chaîne pour utiliser un codage cohérent. la validation plus indulgente dans Chrome lui a permis de fonctionner avec la chaîne de codage mixte, tandis que Firefox et Safari ont rejeté les formats de certificat incohérents.

L'autorité de certification Microsoft a créé des certificats à l'aide du codage printablestring, mais les certificats intermédiaires Cisco Secure Access ont utilisé le codage UTF8STRING. Cette non-correspondance a entraîné l'échec de la validation de la chaîne de certificats de Firefox et Safari au niveau du certificat intermédiaire Cisco.

Autres informations utiles

- Configurer l'accès aux téléconférences Webex dans SWG
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.