Erreur de validation de certificat d'accès sécurisé avec téléchargements du journal du client Splunk

Table des matières

Problème

Les clients Windows exécutant le client Splunk n'ont pas pu télécharger les journaux vers le cloud Splunk en raison d'erreurs de validation de certificat lorsque le trafic a été déchiffré par Cisco Secure Access. Plus de 5 000 sources de journaux Windows n'ont pas pu envoyer de données au cloud Splunk, ce qui a eu un impact sur la réception des journaux. L'erreur spécifique observée dans les journaux du client Splunk était :

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

Le trafic vers la destination *.splunkcloud.com passait par le pare-feu, mais la validation du certificat au niveau de l'application a échoué. La navigation Web vers des sites où le déchiffrement SSL a été activé a continué à fonctionner normalement.

Environnement

- Accès sécurisé Cisco avec décodage SSL/TLS activé
- Clients Windows avec Splunk Universal Forwarder installé
- Destination du nuage Splunk : *.splunkcloud.com
- Plus de 5 000 sources de journaux Windows affectées
- Le client Splunk utilise son propre magasin de certificats, et non le magasin de certificats système Microsoft

Résolution

Le problème a été résolu par la mise en oeuvre d'une politique de contournement de déchiffrement pour le trafic cloud Splunk dans Cisco Secure Access.

Plusieurs mesures ont été prises.

Étape 1: Identifier le problème

Au cours d'une session WebEx, le comportement a été confirmé et reproduit. Les tests ont montré que lorsque le déchiffrement Secure Access était désactivé pour un client ou lorsque le service SWG était désactivé sur le client, les chargements de journaux Splunk ont réussi. Cela a confirmé que le processus de déchiffrement SSL/TLS était à l'origine de l'échec de la validation du certificat.

Étape 2: Créer une liste de destinations

Une liste de destinations a été créée contenant les FQDN et les adresses IP du cloud Splunk pour cibler spécifiquement le trafic destiné aux services cloud Splunk.

Étape 3: Implémenter une stratégie de contournement de décodage

Une stratégie d'accès sécurisé Cisco a été mise en oeuvre pour désactiver le déchiffrement SSL/TLS pour le trafic correspondant à la liste de destination du cloud Splunk. Cette stratégie de contournement a permis aux clients Splunk d'établir des connexions chiffrées directes au cloud Splunk sans interception de certificat par Secure Access.

Étape 4: Validation

Après la mise en oeuvre de la stratégie de contournement du déchiffrement, la validation a confirmé que :

- Les clients Splunk ont réussi à télécharger les journaux
- Le nombre total de clients déclarants dans le cloud Splunk a considérablement augmenté
- Aucune autre erreur de validation de certificat n'a été observée

La gravité du cas a été réduite de 1 à 3 et placée en état de surveillance afin d'observer la poursuite de l'ingestion réussie de journaux.

Motif

La cause principale était que le client Splunk utilise son propre magasin de certificats et ne fait pas confiance au certificat de sous-autorité de certification principale d'accès sécurisé Cisco qui était présenté lors du déchiffrement SSL/TLS. Lorsque Cisco Secure Access a intercepté et décrypté le trafic SSL vers le cloud Splunk, il a recrypté le trafic à l'aide de sa propre autorité de certification. Le processus de validation du certificat du client Splunk a rejeté ce certificat car il n'a pas pu vérifier la chaîne de certificats à une autorité de certification racine de confiance dans son propre magasin de certificats.

L'erreur de validation X.509 spécifique « Unable to get local issuer certificate » (code d'erreur 20) indique que le processus de validation de certificat n'a pas pu localiser l'autorité de certification émettrice dans le magasin de certificats de confiance du client, ce qui a entraîné l'échec de la connexion.

Autres informations utiles

- 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.