

Événements d'authentification VPN d'accès sécurisé avec adresses de serveur AAA link-local

Table des matières

Problème

Lors du test de la fonctionnalité VPN d'accès à distance sécurisé (RA), des événements d'authentification excessifs sont consignés pour des identités qui n'existent pas dans l'organisation du locataire. Les journaux d'authentification affichent plus de 10 000 événements d'authentification VPN RA sur une période de 24 heures, contenant des erreurs AAA telles que « AAALOG_SERVICE_DOWN » et « AAALOG_SERVER_DOWN ». Ces messages d'erreur font référence aux adresses link-local 169.254.x.x en tant que serveur AAA, qui ne sont pas configurées dans le service partagé.

Exemples d'erreurs spécifiques observées dans les journaux :

```
AAALOG_SERVICE_DOWN
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>

AAALOG_SERVER_DOWN
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

L'activité semble être des tentatives d'authentification RADIUS répétées contre le FQDN VPN d'accès sécurisé, ce qui crée un bruit de journal excessif et soulève des préoccupations concernant l'analyse externe ou l'abus potentiel du service VPN.

Environnement

- Plate-forme Cisco Secure Access
- Profil VPN d'accès à distance initialement configuré sans authentification de certificat

- Authentification basée sur RADIUS configurée pour RA VPN
- Configuration de locataire VPN public avec profils VPN détectables

Résolution

La résolution impliquait la compréhension du comportement du flux d'authentification et la mise en oeuvre de l'authentification basée sur les certificats comme stratégie d'atténuation.

Explication technique du comportement observé

Les événements d'authentification excessifs se produisent pour les raisons techniques décrites dans les sections suivantes.

Flux d'authentification sans certificat requis

Lorsque l'authentification de certificat est désactivée et que l'authentification VPN RA RADIUS est utilisée, le système consigne les tentatives d'« échec d'autorisation » car le système vérifie d'abord l'identité du nom d'utilisateur par rapport à la base de données des utilisateurs synchronisés dans Secure Access, et enregistre l'événement « échec d'autorisation ». Ces événements sont attendus comme une première ligne de défense, mais peuvent produire un bruit de journal important lorsque des acteurs externes tentent d'authentifier.

Utilisation des adresses link-local

Les adresses 169.254.x.x visibles dans les journaux sont des adresses de liaison interne/locale utilisées par la tête de réseau VPN RA pour autoriser les sessions entrantes. Ces adresses représentent le comportement interne du système plutôt qu'une mauvaise configuration des serveurs AAA dans le service partagé.

Détection de profil VPN

Lorsqu'un ID de client VPN public est configuré, les profils VPN sont répertoriés dans la liste déroulante de l'interface utilisateur, ce qui permet aux acteurs externes de découvrir plus facilement les profils publics et de les cibler pour les tentatives d'authentification.

Étapes de réduction immédiate

1.- Configurez l'authentification basée sur les certificats. Modifiez le profil VPN RA pour exiger une authentification basée sur un certificat. Lorsque l'authentification de certificat est requise, Secure Access effectue une vérification de certificat plus tôt dans le flux d'authentification. Si le certificat est manquant, le système produit une erreur avant le flux d'authentification standard et les événements « failed authorization » ne sont pas consignés de la même manière.

2.- Valider l'efficacité des mesures d'atténuation. Surveillez les journaux d'authentification après avoir implémenté l'authentification basée sur certificat pour confirmer la réduction des événements d'authentification excessifs. Le passage à l'authentification basée sur les certificats a permis de limiter les attaques et de réduire le bruit des journaux.

Améliorations à long terme

Deux demandes de fonctionnalités ont été créées pour résoudre les problèmes sous-jacents :

- Requête de fonctionnalité 1 : Ajoutez une option permettant de masquer ou d'afficher la liste des groupes de tunnels (profil VPN) lorsqu'un locataire VPN public est ajouté, ce qui réduit la capacité de découverte du profil.
- Demande de fonctionnalité 2 : Ajoutez une option de configuration pour activer ou désactiver la journalisation des tentatives d'autorisation VPN d'annonce de routeur ayant échoué, permettant aux administrateurs de contrôler le niveau de détail des journaux.

En outre, un document public est créé pour expliquer les événements consignés et le comportement d'authentification afin d'aider les administrateurs à comprendre le fonctionnement normal du système.

Motif

La cause première des événements d'authentification excessifs est la combinaison de profils VPN détectables dans des configurations de locataires publics et le comportement du flux d'authentification lorsque l'authentification basée sur certificat n'est pas requise. Lorsque l'authentification RADIUS est utilisée sans certificat requis, le système consigne toutes les tentatives d'« échec d'autorisation » dans le cadre de sa stratégie de sécurité, y compris les tentatives d'acteurs externes qui découvrent les profils VPN. Les adresses link-local dans les journaux représentent un comportement interne normal du système pour le processus d'autorisation de tête de réseau VPN RA, et non des erreurs de configuration.

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.