

Fonction ISE RCM entraînant la suppression des terminaux pendant l'authentification basée sur les certificats

Table des matières

Problème

Lors d'une migration de JAMF vers Intune MDM pour les périphériques macOS, Cisco ISE supprime ou fusionne de manière inattendue les enregistrements de terminaux et modifie les affectations de groupes d'identité de terminaux lors de l'authentification EAP-TLS.

Les points d'extrémité affectés sont déplacés du groupe d'identité DB_Authorized_Devices vers Profiled déclenchant des événements CoA avec la raison « Delegation of Endpoint ». Cela entraîne la suppression des terminaux de la base de données interne ISE et entraîne des pannes d'authentification pour les périphériques affectés. Le problème se produit lorsque les périphériques passent d'une connexion sans fil à une connexion câblée à l'aide du même certificat contenant les champs URI de l'autre nom du sujet (SAN) que l'ISE interprète comme GUID pour la fonctionnalité MAC aléatoire et changeante (RCM).

Environnement

- Cisco Identity Services Engine (ISE) version 3.2
- Terminaux macOS utilisant l'authentification EAP-TLS
- Authentification basée sur certificat avec champs URI SAN contenant des identifiants de périphériques
- Périphériques commutant entre les connexions réseau filaires et sans fil
- Migration MDM de JAMF vers Microsoft Intune
- Fonction RCM (Random and Changing MAC) activée par défaut dans ISE 3.2

- Terminaux gérés via l'API REST avec des attributs personnalisés

Résolution

Le problème est causé par la fonctionnalité RCM d'ISE 3.2, qui fusionne les enregistrements de point de terminaison en fonction des champs URI SAN du certificat. Deux options de résolution sont disponibles.

Option 1: Désactiver la fonction RCM (recommandé avec prudence)

Étape 1: Accès à l'interface ISE Swagger API

Accédez à Administration > Settings > API Settings et cliquez sur le lien /swagger-ui.

Étape 2: Vérifier les paramètres LSD actuels

Dans l'interface Swagger, recherchez LSD Settings et exécutez une requête GET pour afficher la configuration actuelle :

```
GET /api/v1/lsd/settings
```

Étape 3: Modifier les paramètres du RCM

Exécutez une requête PUT avec ce corps de requête pour désactiver le RCM :

```
{  
  "enableEPO": true,
```

```
"enableRCM": false  
}
```

Étape 4: Vérification de la modification de configuration

Exécutez à nouveau la requête GET pour confirmer que RCM est désactivé et que LSD reste activé.

Étape 5: Exécuter des scripts de nettoyage

Exécutez l'opération de script recommandée pour corriger les écarts d'attribut après la désactivation du RCM. Surveillez l'infrastructure afin de détecter les éventuels incidents au cours de ce processus.



Mise en garde : Possible. Les détails mentionnés ici semblent contenir des procédures ou des commandes qui pourraient avoir un impact significatif si elles étaient exécutées. Veuillez vous assurer que les procédures ou commandes ont été évaluées par un expert ou une unité commerciale avant d'exécuter ou de recommander.

Option 2: Modifier les stratégies d'autorisation

Ajuster les ensembles de stratégies pour tenir compte du comportement du RCM en créant une logique d'autorisation distincte pour les flux d'authentification filaire et sans fil, afin de s'assurer que les points d'extrémité fusionnés reçoivent les décisions d'accès appropriées en fonction du type de connexion plutôt que de l'appartenance au groupe d'identité seul.

Traitement des URI SAN de certificat

ISE traite les champs URI SAN de certificat en utilisant une logique spécifique pour extraire les GUID. Pour les certificats contenant des segments Microsoft Entra ID, ISE supprime les segments d'identité transitoires à l'aide du modèle d'expression régulière :

tag:[a-zA-Z0-9.,-]+:sid:S-[0-9-]+[: ,]?

Exemples de traitement d'URI SAN :

- Entrée: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- Stocké dans la session : "ID:Meraki:GUID:673288144292101809"

Motif

La fonctionnalité RCM (Random and Changing MAC) activée par défaut dans ISE 3.2 interprète les champs URI SAN de certificat comme des GUID pour l'identification des terminaux. Lorsque des périphériques utilisant le même certificat se connectent via des interfaces sans fil et câblées, le RCM fusionne les enregistrements de point d'extrémité en fonction du GUID partagé. Au cours de ce processus de fusion, les attributs du point d'extrémité sans fil sont migrés vers le point d'extrémité câblé et l'entrée MAC sans fil est supprimée de la base de données de points d'extrémité. Ce comportement se produit avant les sondes CoA ou DHCP et entraîne la perte d'attributs personnalisés et d'affectations de groupes d'identité qui ont été configurés à l'origine via l'API REST. Le processus de fusion ne conserve pas les attributs personnalisés qui ne font pas partie des stratégies de profilage, ce qui entraîne la réinitialisation de l'identité du point de terminaison et des échecs d'authentification ultérieurs.

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.