Mettre à jour le certificat de parapluie DNS pour qu'il fonctionne en octobre 2024

Table des matières

Introduction

Informations générales

Informations sur les défauts

Fixe Relâché

- Versions CCO

Matrice de correction

- 1. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.5.x ou antérieure en mode contrôleur
  - Automatisé
  - Manuel
- 2. Périphériques Cisco exécutant le logiciel Cisco IOS XE versions 17.6.x à 17.8.x en mode contrôleur
  - Automatisé
  - Manuel
- 3. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.9.5a en mode contrôleur
- 4. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.9.6 en mode contrôleur
- 5. Périphériques Cisco équipés du logiciel Cisco IOS XE version 17.12.3a en mode contrôleur
- 6. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.12.4 en mode contrôleur

Introduction

Ce document décrit comment résoudre le problème DNS Umbrella où les routeurs SD-WAN utilisent le certificat expiré au lieu du nouveau.

Informations générales

Le certificat numérique utilisé par les routeurs SD-WAN Cisco Catalyst pour s'enregistrer à l'aide de la méthode d'authentification API Key/Secret avec Cisco Umbrella DNS a expiré le 30 septembre 2024. Les routeurs SD-WAN Cisco dont le certificat a expiré ne pourront pas s'enregistrer auprès du service Cisco Umbrella DNS. Ce problème ne s'applique pas à l'authentification basée sur les jetons pour l'enregistrement du DNS Umbrella.

Consultez le certificat Cisco Umbrella DNS expirant le 30 septembre 2024, dans l'avis de champ FN74166 pour plus de détails.

Les périphériques SD-WAN affectés dont le certificat CA racine de parapluie a expiré ne peuvent pas établir de connexions sécurisées avec Cisco Umbrella DNS pour l'enregistrement des périphériques. Comme le périphérique n'est pas enregistré auprès du service DNS Umbrella, les

requêtes DNS de l'utilisateur final ne sont pas redirigées vers le serveur de domaine Umbrella par la périphérie SD-WAN pour l'application de la stratégie de sécurité DNS. La requête DNS des utilisateurs finaux derrière la périphérie SD-WAN ne sera pas abandonnée et sera traitée par le serveur de domaine DNS configuré sur les périphériques des utilisateurs finaux.

Informations sur les défauts

Le certificat a été mis à jour dans le cadre du bogue Cisco ID CSCwi43360
: le certificat expire en septembre 2024 pour l'enregistrement de la sécurité DNS sur le cloud Umbrella. (fixé dans 17.9.6, 17.12.4, 17.15.1a)

Même lorsque le certificat est mis à jour, la connexion SSL ne parvient pas à s'établir, ce qui fait partie de l'ID de bogue Cisco CSCwm73365
: La connexion SSL échoue malgré umbrella_root_ca.ca avec le dernier certificat présent sur le périphérique. (fixé au point 17.6.8a)

Fixe Relâché

Versions CCO

Libérer	17.6.8 bis

Matrice de correction

Versions	Étapes de correction recommandées par Cisco
17.3.x/17.4.x/17.5.x	Suivez les étapes de la section 1. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.5.x ou antérieure en mode contrôleur
17.6.1 à 17.6.7, 17.7.x, 17.8.x	Suivez les étapes de la section 2. Périphériques Cisco exécutant le logiciel Cisco IOS XE versions 17.6.x à 17.8.x en mode contrôleur
17.6.8 bis	Le problème d'expiration du certificat Umbrella DNS est résolu dans cette version.
17.9.1 à 17.9.4, 17.10.x, 17.11.x, 17.12.1 à 17.12.2, 17.13.x, 17.14.x, 17.15.1a	Utilisez Umbrella DNS Cert Script pour la copie automatique des certificats vers les périphériques Edge. Reportez-vous au fichier readme sur le GIT pour connaître les étapes à suivre pour exécuter le script.
17.9.5 bis	Suivez les étapes de la section 3
17.9.6	Suivez les étapes de la section 4
17.12.3 bis	Suivez les étapes de la section 5
17.12.4	Suivez les étapes de la section 6

1. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.5.x ou antérieure en mode contrôleur

Utilisez les options de conversion pour installer le nouveau certificat Umbrella RootCA.

Automatisé

1. Pour SD-WAN Manager 20.9.1 ou version ultérieure, utilisez le script Umbrella DNS Cert pour une copie automatisée du certificat vers les périphériques de périphérie à partir de

vManage.
2. Script de certification DNS Umbrela
3. Reportez-vous au fichier readme sur le GIT pour les étapes détaillées d'utilisation du script.
4. Une fois le certificat RootCA copié sur le périphérique, rechargez le routeur pour terminer le processus d'installation.

Manuel

1. Téléchargez le nouveau certificat non expiré depuis le site Web New Umbrella Certificate et placez-le sur un périphérique qui a accès au(x) routeur(s) concerné(s) dans la superposition SD-WAN.
2. Entrez la commande scp de Linux ou un mécanisme similaire pour effectuer une copie sécurisée du fichier à partir du périphérique de téléchargement sur chaque routeur concerné.

   Exemple :

   scp ./isrgrootx1.pem <Nom d'utilisateur>@<IPpériphérie>:trustidrootx3_ca.ca

   Remplacez <Username> par un utilisateur admin et <EdgeIP> par l'adresse IP du routeur concerné.

3. Une fois le certificat RootCA copié sur le périphérique, rechargez le routeur pour terminer le processus d'installation.

2. Périphériques Cisco exécutant le logiciel Cisco IOS XE versions 17.6.x à 17.8.x en mode contrôleur

Utilisez les options de conversion pour installer le nouveau certificat Umbrella RootCA.

Automatisé

1. Pour SD-WAN Manager 20.9.1 ou version ultérieure, utilisez le script Umbrella DNS Cert pour une copie automatisée du certificat vers les périphériques de périphérie à partir de vManage.
2. Script de certification DNS Umbrella
3. Reportez-vous au fichier readme sur le GIT pour les étapes détaillées d'utilisation du script.
4. Une fois le certificat RootCA copié sur le périphérique, rechargez le routeur pour terminer le processus d'installation.

Manuel

1. Téléchargez le nouveau certificat non expiré depuis le site Web New Umbrella Certificate et placez-le sur un périphérique qui a accès au(x) routeur(s) concerné(s) dans la superposition SD-WAN.
2. Entrez la commande scp de Linux ou un mécanisme similaire pour effectuer une copie sécurisée du fichier à partir du périphérique de téléchargement sur chaque routeur affecté.

Exemple :

scp ./isrgrootx1.pem admin@<IP de périphérie> : trustidrootx3_ca_092024.ca

Remplacez <EdgeIP> par l'adresse IP du routeur concerné.

3. Une fois le certificat RootCA copié sur le périphérique, rechargez le routeur pour terminer le processus d'installation

3. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.9.5a en mode contrôleur

Utilisez les options de conversion pour installer le nouveau certificat Umbrella RootCA comme expliqué dans cette section, pour la plupart des plates-formes il y a une SMU HOT disponible avec le correctif. Vous avez également la possibilité d'exécuter le script mentionné pour installer le nouveau certificat Umbrella RootCA.

1. La SMU HOT s'applique à ces plates-formes - «SMU sans problème/recommandé, la connexion SSL échoue malgré umbrella_root_ca.ca avec le dernier certificat présent sur le périphérique» :

Routeur à services intégrés 4431
Routeur à services intégrés 4451-X

Routeur ASR 1001-X
Routeurs virtuels
Routeur à services intégrés 4331
Routeur à services intégrés 4221
Routeur à services intégrés 4351
Plate-forme de périphérie Catalyst 8500L
Routeur ASR 1001-HX
Routeur à services intégrés 4321

Plate-forme de périphérie Catalyst 8500

Routeur à services intégrés 4461

2. Alternative à SMU, exécutez le script Umbrella DNS Cert Script Consultez le fichier readme sur le GIT pour les étapes détaillées pour utiliser le script.

Option Script uniquement pour :
Routeur ASR1002-X

Plate-forme de périphérie Catalyst 8300

Gamme ISR 1000 exécutant Cisco IOS XE SD-WAN

4. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.9.6 en mode contrôleur

1. La SMU HOT s'applique à ces plates-formes - « SMU sans problème/recommandé, la connexion SSL échoue malgré umbrella_root_ca.ca avec le dernier certificat présent sur le périphérique » :

   Routeur à services intégrés 4221
   Routeur à services intégrés 4321
   Routeur à services intégrés 4451-X
   Plate-forme de périphérie Catalyst 8500
   Routeur à services intégrés 4431
   Routeurs virtuels
   Routeur à services intégrés 4461
   Routeur à services intégrés 4331
   Routeur à services intégrés 4351
   Routeur ASR 1001-HX
   Routeur ASR 1001-X
   Plate-forme de périphérie Catalyst 8500L

3. Alternative à SMU, exécutez le script Umbrella DNS Cert Script Consultez le fichier readme sur le GIT pour les étapes détaillées pour utiliser le script.

Option Script uniquement pour :

Routeur ASR1002-X

Plate-forme de périphérie Catalyst 8300

Gamme ISR 1000 exécutant Cisco IOS XE SD-WAN

5. Périphériques Cisco équipés du logiciel Cisco IOS XE version 17.12.3a en mode contrôleur

1. La SMU HOT s'applique à ces plates-formes - « SMU sans problème/recommandé, la connexion SSL échoue malgré umbrella_root_ca.ca avec le dernier certificat présent sur le périphérique » :

   Routeur à services intégrés 4221
   Plate-forme de périphérie Catalyst 8300
   Routeur à services intégrés 4331
   Routeur à services intégrés 4461
   Routeur à services intégrés 1100
   Routeur à services intégrés 4351
   Routeur à services intégrés 4321
   Routeur à services intégrés 4431
   Routeurs virtuels
   Routeur à services intégrés 4451-X

   Plate-forme de périphérie Catalyst 8500L
   Plate-forme de périphérie Catalyst 8500

Routeur ASR 1001-HX

2. Alternative à SMU, exécutez le script Script de certification DNS Umbrella

Reportez-vous au fichier readme sur le GIT pour les étapes détaillées d'utilisation du script.

6. Périphériques Cisco exécutant le logiciel Cisco IOS XE version 17.12.4 en mode contrôleur

1. La SMU HOT s'applique à ces plates-formes - « SMU sans problème/recommandé, la connexion SSL échoue malgré umbrella_root_ca.ca avec le dernier certificat présent sur le périphérique » :

Plate-forme de périphérie Catalyst 8500
Routeur ASR 1001-HX
Routeur à services intégrés 4331
Routeur à services intégrés 4321
Routeur à services intégrés 4221
Routeurs virtuels
Routeur à services intégrés 4351
Routeur à services intégrés 4451-X
Routeur à services intégrés 4461
Plate-forme de périphérie Catalyst 8300
Routeur ASR 1002-HX
Routeur à services intégrés 4431

Routeur à services intégrés 1100

Plate-forme de périphérie Catalyst 8500L

2. L'alternative à SMU est d'exécuter le script Umbrella DNS Cert Script Consultez le fichier readme sur le GIT pour les étapes détaillées pour utiliser le script.

⚠ Attention : les enregistrements de DNS parapluie à partir des périphériques continuent à fonctionner tant qu'il n'y a pas de redémarrage du périphérique ou pas de nouveaux enregistrements.

⚠ Attention : si la configuration de parapluie est supprimée et réappliquée, cela déclenche le réenregistrement du DNS de parapluie. Tant que ce processus n'est pas suivi, le DNS parapluie fonctionne correctement.

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.