Recommandations contre les attaques par pulvérisation de mot de passe affectant les services VPN d'accès à distance

Table des matières

Introduction

Ce document décrit les recommandations à prendre en compte contre les échecs d'allocation de jeton hostcan dans Secure Firewall, dérivés d'attaques par pulvérisation de mot de passe.

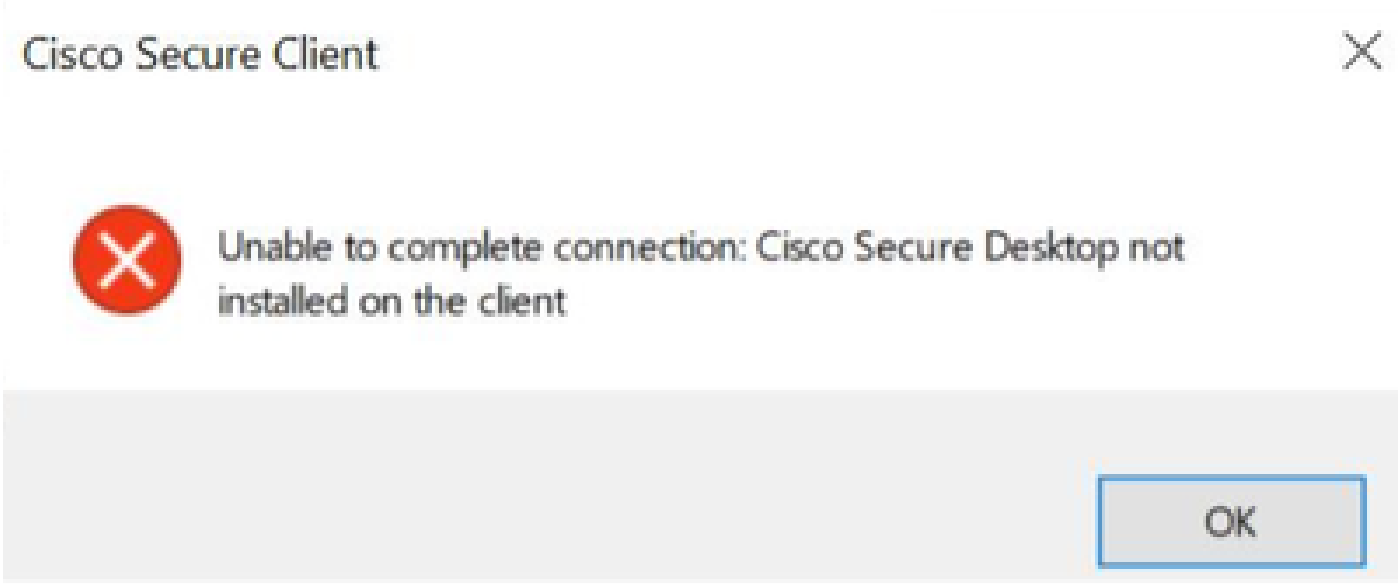
Informations générales

Lors d'une tentative d'établissement d'une connexion RAVPN à l'aide de Cisco Secure Client (AnyConnect), les utilisateurs peuvent rencontrer par intermittence un message d'erreur indiquant "Unable to complete connection. Cisco Secure Desktop n'est pas installé sur le client.". Ce comportement se produit généralement en cas d'échec de l'allocation d'un jeton de balayage d'hôte par la tête de réseau VPN, soit un dispositif de sécurité adaptatif (ASA) Cisco Secure Firewall, soit un dispositif de défense contre les menaces (FTD). En particulier, cet échec d'allocation est corrélé avec des cas d'attaques en force ciblant l'infrastructure du pare-feu sécurisé et est actuellement traité de la manière la plus urgente sous l'ID de bogue Cisco CSCwj45822.

Comportements observés

Impossible d'établir des connexions VPN avec Cisco Secure Client (AnyConnect) lorsque la position du pare-feu (HostScan) est activée

Lorsque vous tentez d'établir une connexion VPN à l'aide de Cisco Secure Client (AnyConnect), les utilisateurs peuvent rencontrer par intermittence un message d'erreur indiquant « Unable to complete connection. Cisco Secure Desktop n'est pas installé sur le client. Ce problème empêche la réussite du processus de connexion VPN.



Remarque : ce comportement spécifique se produit uniquement lorsque la position du pare-feu (HostScan) est activée en tête de réseau, quelle que soit la version du client sécurisé ou AnyConnect utilisée.

Épuisement du jeton Hostscan

La tête de réseau VPN Cisco Secure Firewall Adaptive Security Appliance (ASA) ou Threat Defense (FTD) présente des symptômes d'échecs d'allocation de jeton hostscan. Pour le vérifier, exécutez la commande debug menu webvpn 187 0.

<#root>

```
ASA# debug menu webvpn 187 0
Allocated Hostscan token = 1000
```

Hostscan token allocate failure = xxx - - - - > Increments

Remarque : la survenue de ce problème est une conséquence des attaques. Le problème est actuellement traité de la manière la plus urgente sous l'ID de bogue Cisco CSCwj4582.

Nombre inhabituel de demandes d'authentification

La tête de réseau VPN Cisco Secure Firewall ASA ou FTD présente des symptômes d'attaques par pulvérisation de mot de passe avec 100 000 ou des millions de tentatives d'authentification rejetées.

Remarque : ces tentatives inhabituelles d'authentification peuvent être dirigées vers la base de données LOCAL ou vers des serveurs d'authentification externes.

La meilleure façon de détecter ceci est en regardant le syslog. Recherchez un nombre inhabituel d'ID syslog ASA suivants :

- %ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database :

user

= *admin* : user

IP

= *x.x.x.x*

- %ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

- %ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.

Le nom d'utilisateur est toujours masqué jusqu'à ce que la commande no logging hide username soit configurée sur l'ASA.

Remarque : ceci vous permet de vérifier si des utilisateurs valides sont générés ou connus par des adresses IP incorrectes. Cependant, soyez prudent car les noms d'utilisateurs seront visibles dans les journaux.

Pour vérifier, connectez-vous à l'interface de ligne de commande (CLI) ASA ou FTD, exécutez la commande show aaa-server, et recherchez un nombre inhabituel de demandes d'authentification tentées et rejetées à l'un des serveurs AAA configurés :

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
```

Number of authentication requests 2228536 - - - - - >>>> Unusual increments

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
```

Number of rejects 2225363 - - - - - >>>> Unusual increments / Unusual rejection rate

```
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
```

```
Number of unrecognized responses 0
```

Recommandations

Bien qu'il n'existe actuellement aucune solution unique pour éliminer complètement le risque, vous pouvez passer en revue et appliquer les pratiques recommandées suivantes, qui sont conçues pour aider à réduire la probabilité d'occurrence et diminuer l'impact de ces attaques en force sur vos connexions RAVPN.

1. Activer la journalisation

La journalisation est un élément essentiel de la cybersécurité qui implique l'enregistrement des événements se produisant dans un système. L'absence de journaux détaillés laisse des lacunes dans la compréhension, ce qui empêche une analyse claire de la méthode d'attaque. Il est recommandé d'activer la journalisation sur un serveur syslog distant pour améliorer la corrélation et l'audit des incidents réseau et de sécurité sur divers périphériques réseau.

Pour plus d'informations sur la configuration de la journalisation, reportez-vous aux guides suivants spécifiques à la plate-forme :

Logiciel Cisco ASA :

- Guide d'utilisation du pare-feu ASA sécurisé
- Chapitre Journalisation du Guide de configuration CLI des opérations générales de la gamme Cisco Secure Firewall ASA

Logiciel Cisco FTD :

- Configurer la connexion au FTD via le centre de gestion des pare-feu (FMC)
- Section Configure Syslog du chapitre Platform Settings du Guide de configuration des périphériques de Cisco Secure Firewall Management Center
- Configuration et vérification de Syslog dans le Gestionnaire de périphériques Firepower
- Section Configuration des paramètres de journalisation système du chapitre Paramètres système du Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager

---

Remarque : les ID de message Syslog nécessaires pour vérifier les comportements décrits dans ce document (113015, 113005 & 716039), doivent être activés au niveau informatif (6). Ces ID font partie des classes de journalisation 'auth' et 'webvpn'.

---

2. Appliquer des mesures de renforcement pour le VPN d'accès à distance

Pour atténuer l'impact de ces attaques, mettez en oeuvre les mesures de renforcement suivantes :

1. Désactiver l'authentification AAA dans les profils de connexion DefaultWEBVPN et DefaultRAGroup (étape par étape : ASA | FTD géré par FMC).
2. Désactivez la position de pare-feu sécurisé (Hostscan) à partir des groupes DefaultWEBVPNGroup et DefaultRAGroup (étape par étape : ASA | FTD géré par FMC).
3. Désactivez les alias de groupe et activez les URL de groupe dans le reste des profils de connexion (étape par étape : ASA | FTD géré par FMC).

Remarque : si vous avez besoin d'une assistance avec FTD gérée par le biais de la gestion locale des périphériques pare-feu (FDM), contactez le centre d'assistance technique (TAC) pour obtenir des conseils d'experts.

Pour plus de détails, veuillez vous reporter au guide Implémenter des mesures de renforcement pour le VPN AnyConnect Secure Client.

3. Bloquer les tentatives de connexion provenant de sources malveillantes

Afin d'empêcher les tentatives de connexion provenant de sources non autorisées, vous pouvez implémenter l'une des options suivantes :

Implémenter des ACL au niveau de l’interface

Implémentez une liste de contrôle d'accès au niveau de l'interface sur l'ASA/FTD pour filtrer les adresses IP publiques non autorisées et les empêcher d'initier des sessions VPN distantes.

Utiliser la commande « shun »

Il s'agit d'une approche simple pour bloquer une adresse IP malveillante, mais elle doit être effectuée manuellement. Veuillez lire la section Configuration alternative pour bloquer les attaques pour le pare-feu sécurisé en utilisant la commande « shun » pour plus de détails.

Configurer la liste de contrôle d’accès Control-plane

Implémentez une liste de contrôle d'accès du plan de contrôle sur l'ASA/FTD pour filtrer les adresses IP publiques non autorisées et les empêcher d'initier des sessions VPN distantes. Configurez les stratégies de contrôle d'accès au plan de contrôle pour Secure Firewall

Threat Defense et ASA.

Remarque : Cisco Talos a publié une liste d'adresses IP et d'identifiants associés à ces attaques. Un lien vers leur dépôt GitHub se trouve dans la section « IOC » de leur avis. Il est important de noter que les adresses IP source de ce trafic sont susceptibles de changer. Par conséquent, vous devez consulter les journaux de sécurité (syslog) pour identifier les adresses IP problématiques. Lors de l'identification, l'une des 3 options peut être utilisée pour les bloquer.

Implémentations de durcissement supplémentaires pour RAVPN

Les recommandations fournies jusqu'à présent visent à réduire le risque et l'impact des attaques sur les services RAVPN. Cependant, vous pouvez envisager des contre-mesures supplémentaires qui nécessitent des modifications supplémentaires dans vos déploiements pour renforcer la sécurité de votre déploiement VPN d'accès à distance, telles que l'adoption de l'authentification basée sur certificat pour RAVPN. Reportez-vous au document Implement Hardening Measures for Secure Client AnyConnect VPN pour obtenir des instructions de configuration détaillées.

Additional Information

- Procédures d'investigation de Cisco ASA pour les premiers intervenants
- Procédures d'investigation scientifique de Cisco Firepower Threat Defense pour les premiers intervenants
- Avis sur les menaces Cisco Talos
- Pour obtenir de l'aide supplémentaire, veuillez contacter le Centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.

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.