Recommandations contre les attaques par pulvérisation de mot de passe visant les services VPN d'accès à distance dans Secure Firewall

Table des matières

Introduction

Ce document décrit les recommandations à prendre en compte contre les attaques par mot de passe visant les services VPN d'accès à distance dans Secure Firewall.

Informations générales

Les attaques par pulvérisation de mots de passe sont un type d'attaque en force où un pirate tente d'obtenir un accès non autorisé à plusieurs comptes d'utilisateurs en essayant systématiquement quelques mots de passe couramment utilisés sur de nombreux comptes. Les attaques réussies par pulvérisation de mots de passe peuvent entraîner un accès non autorisé aux informations sensibles, des violations de données et des atteintes potentielles à l'intégrité du réseau

En outre, ces attaques, même si elles échouent dans leur tentative d'accès, peuvent consommer des ressources informatiques du pare-feu sécurisé et empêcher les utilisateurs valides de se connecter aux services VPN d'accès à distance.

Comportements observés

Lorsque votre pare-feu sécurisé est la cible d'attaques par mot de passe dans les services VPN d'accès à distance, vous pouvez identifier ces attaques en surveillant les journaux système et en utilisant des commandes show spécifiques. Les comportements les plus courants à rechercher sont les suivants :

Nombre inhabituel de demandes d'authentification rejetées

La tête de réseau VPN Cisco Secure Firewall ASA ou FTD présente des symptômes d'attaques par pulvérisation de mot de passe avec un taux inhabituel (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

Examiner et appliquer les recommandations suivantes.

1. Activez 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 :

- Utiliser le guide pour sécuriser le pare-feu pour appareil de sécurité adaptable
- 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. Configurez les fonctionnalités de détection des menaces ou les mesures de

renforcement pour le VPN d'accès à distance.

Pour réduire l'impact et la probabilité de ces attaques en force sur vos connexions RAVPN, vous pouvez passer en revue et appliquer les options de configuration suivantes :

Option 1 (préférable) : configurez la détection des menaces pour les services VPN d'accès à distance.

Les fonctionnalités de détection des menaces pour les services VPN d'accès à distance vous permettent de vous protéger contre ce type d'attaques en bloquant automatiquement l'hôte (adresse IP) qui dépasse les seuils configurés, afin d'empêcher toute nouvelle tentative jusqu'à ce que vous supprimiez manuellement la désactivation de l'adresse IP.

Ces fonctions de détection des menaces sont actuellement prises en charge dans les versions de Cisco Secure Firewall suivantes :

Logiciel ASA :

- train version 9.16 -> pris en charge dans le train 9.16(4)67 et les versions plus récentes dans ce train spécifique
- train version 9.18 -> pris en charge dans le train 9.18(4)40 et les versions plus récentes dans ce train spécifique
- train version 9.20 -> pris en charge dans le train 9.20(3) et les versions plus récentes dans ce train spécifique

Logiciel FTD :

- train de versions 7.0 -> pris en charge dans la version 7.0.6.3 et les versions ultérieures de ce train spécifique.

Remarque : ces fonctionnalités ne sont actuellement pas prises en charge dans les versions 7.1, 7.2, 7.3 ou 7.4. Ce document est mis à jour dès qu'ils sont disponibles.

Pour obtenir des informations détaillées et des conseils de configuration, reportez-vous aux documents suivants :

- Configuration sur Secure Firewall ASA : configurez la détection des menaces pour le VPN d'accès à distance sur Secure Firewall ASA.
- Configuration sur Secure Firewall FTD : configuration de la détection des menaces pour les services VPN d'accès à distance sur Secure Firewall Threat Defense

Option 2 : appliquer des mesures de renforcement pour le VPN d'accès à distance.

Si les fonctions de détection des menaces pour les services VPN d'accès à distance ne sont pas prises en charge dans votre version Secure Firewall, mettez en oeuvre toutes les mesures de sécurisation suivantes afin d'atténuer l'impact de ces attaques :

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 via la gestion locale des 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.

Option 3 : bloquer manuellement 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 :

- Utilisez 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.

- Configurez la liste de contrôle d'accès du plan de contrôle :

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

---

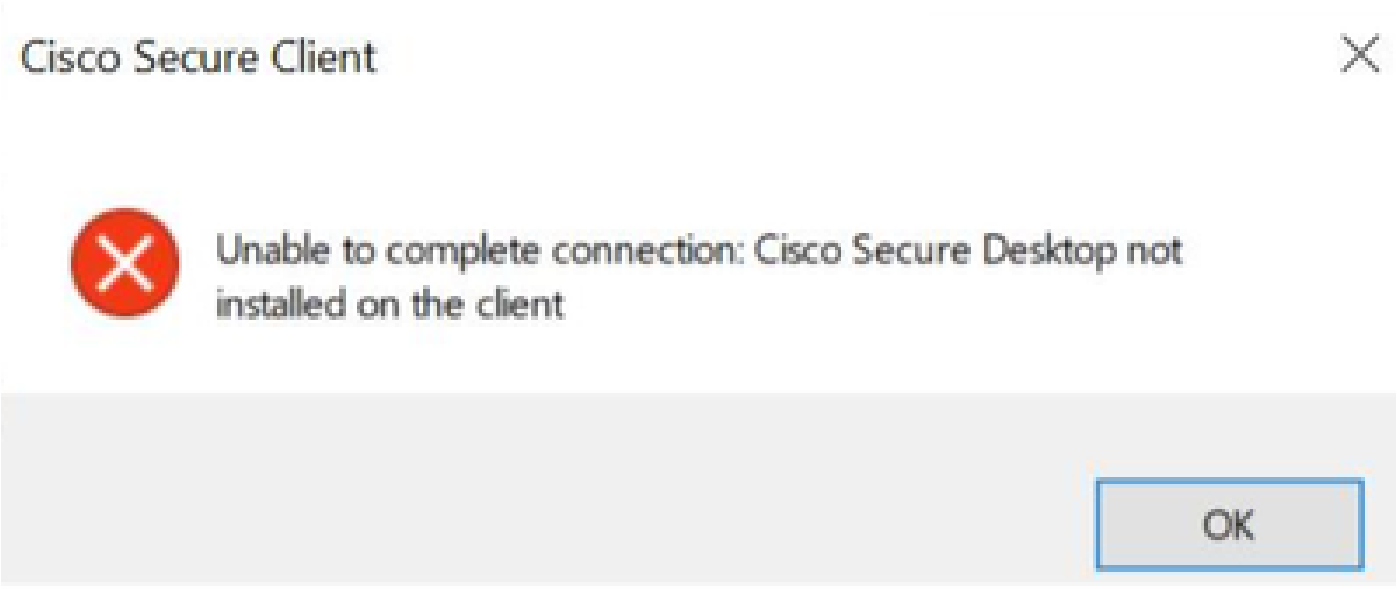
adresses IP problématiques. Lors de l'identification, l'une des 3 options peut être utilisée pour les bloquer.

Comportements connexes

Certains symptômes peuvent apparaître lorsque le pare-feu sécurisé est la cible d'attaques par pulvérisation de mot de passe. Pour résoudre ces problèmes, il faut envisager de mettre en oeuvre les recommandations fournies dans le présent document.

Symptôme latéral 1 : impossible d'établir des connexions VPN avec Cisco Secure Client (AnyConnect) lorsque la position du pare-feu (HostScan) est activée

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 d'allocation d'un jeton de balayage d'hôte par la tête de réseau VPN, qu'il s'agisse d'un pare-feu ASA ou FTD Cisco. Notamment, cet échec d'allocation est corrélé avec des cas d'attaques en force ciblant l'infrastructure du pare-feu sécurisé et empêche la réussite du processus de connexion VPN. Ce comportement a été suivi et résolu via l'ID de bogue Cisco CSCwj45822.



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.

Pour vérifier si la tête de réseau VPN Cisco Secure Firewall ASA ou FTD présente des symptômes d'échecs d'allocation de jeton hostscan, 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. Ce comportement a été suivi et résolu via l'ID de bogue Cisco CSCwj45822.

Pour résoudre ce problème, pensez à mettre en oeuvre les recommandations fournies dans ce document.

Implémentations de durcissement supplémentaires pour RAVPN

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 : Coordonnées du service d'assistance Cisco à l'échelle mondiale.

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.