Atténuer les attaques par pulvérisation de mot de passe sur le pare-feu sécurisé VPN distant

Table des matières

Introduction

Informations générales

Comportements observés

- Nombre inhabituel de demandes d'authentification rejetées

Recommandations

- 1. Activer la journalisation
- 2. Configurer les fonctionnalités de détection des menaces ou les mesures de renforcement pour le VPN d'accès à distance
  - Option 1 (recommandée) : Configurer la détection des menaces pour les services VPN d'accès à distance
  - Option 2: Appliquer des mesures de renforcement pour le VPN d'accès distant

Comportements connexes

- ID de bogue Cisco CSCwj45822 : Vulnérabilité de force de déni de service du VPN d'accès à distance Cisco ASA et FTD (CVE-2024-20481)

Additional Information

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 dans laquelle un pirate tente d'obtenir un accès non autorisé à plusieurs comptes d'utilisateurs en utilisant systématiquement quelques mots de passe couramment utilisés sur de nombreux comptes. Des attaques par pulvérisation de mots de passe réussies peuvent entraîner un accès non autorisé à des 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 exécutant 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 de tentatives d'authentification rejetées.

Remarque : Ces tentatives inhabituelles d'authentification peuvent être dirigées soit vers la base de données LOCALE, soit 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 : Cela permet de vérifier si des utilisateurs valides sont générés ou connus par des adresses IP incorrectes. Cependant, soyez prudent car les noms d'utilisateur sont visibles dans les journaux.

Pour vérifier, connectez-vous à l'interface de ligne de commande (CLI) ASA ou FTD et exécutez la commande show aaa-server. Recherchez un nombre inhabituel de tentatives et de refus de demandes d'authentification 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 décrites ci-dessous :

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 et 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 spécifiques à la plate-forme suivants :

Logiciel Cisco ASA :

- Guide du pare-feu ASA sécurisé
- Guide de journalisation de la 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 sont nécessaires pour vérifier les comportements décrits dans ce document (113015, 113005 & 716039). Ils doivent être activés au niveau informationnel (6) car ces ID font partie des classes de journalisation 'auth' et 'webvpn'.

---

2. Configurer 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 (recommandée) : Configurer 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 permettent d'empêcher les attaques DoS (Denial of Service) à partir d'adresses IPv4 en bloquant automatiquement l'hôte (adresse IP) qui dépasse les seuils configurés pour empêcher toute nouvelle tentative jusqu'à ce que vous supprimiez manuellement la désactivation de l'adresse IP. Des services distincts sont disponibles pour ces types d'attaques :

- Tentatives répétées d'authentification échouées vers les services VPN d'accès à distance (attaques d'analyse de nom d'utilisateur/mot de passe en force).
- Le client lance des attaques lorsque le pirate démarre, mais ne termine pas les tentatives de connexion à une tête de réseau VPN d'accès à distance répétées à partir d'un hôte unique.

- Connection tente d'activer des services VPN d'accès à distance non valides lorsque des pirates tentent de se connecter à des groupes de tunnels intégrés spécifiques destinés uniquement au fonctionnement interne du périphérique. Les terminaux légitimes ne doivent jamais tenter de se connecter à ces groupes de tunnels.

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 à partir de la version 9.16(4)67 et des versions plus récentes dans ce train spécifique.
- train version 9.17 -> pris en charge à partir de la version 9.17(1)45 et des versions plus récentes dans ce train spécifique.
- train version 9.18 -> pris en charge à partir de la version 9.18(4)40 et des versions plus récentes dans ce train spécifique.
- train version 9.19 -> pris en charge à partir de la version 9.19(1).37 et des versions plus récentes dans ce train spécifique.
- train version 9.20 -> pris en charge à partir de la version 9.20(3) et des versions plus récentes dans ce train spécifique.
- 9.22 version train -> prise en charge à partir de 9.22(1.1) et de toute version plus récente.

Logiciel FTD :

- train de versions 7.0 -> pris en charge à partir de la version 7.0.6.3 et des versions plus récentes dans ce train spécifique.
- 7.2 version train -> prise en charge à partir de la version 7.2.9 et des versions ultérieures dans cette version spécifique.
- 7.4 version train -> prise en charge à partir de la version 7.4.2.1 et des versions ultérieures dans cette version spécifique.
- 7.6 version train -> prise en charge à partir de 7.6.0 et des versions ultérieures.

Remarque : Ces fonctionnalités ne sont actuellement pas prises en charge dans les versions 7.1 ou 7.3.

Pour obtenir des informations détaillées et une assistance de configuration, reportez-vous aux guides de documentation suivants :

- Configuration sur Secure Firewall ASA : configuration de la détection des menaces pour le VPN d'accès à distance sur Secure Firewall ASA
- Configuration sur Secure Firewall FTD géré par FMC : configuration de la détection des menaces pour les services VPN d'accès à distance sur Secure Firewall Management Center
- Configuration sur le pare-feu sécurisé FTD géré par FDM : Configurer la détection des menaces pour les services VPN d'accès à distance sur le Gestionnaire de périphériques Secure Firewall

Option 2: Appliquer des mesures de renforcement pour le VPN d'accès distant

---

Remarque : Ces mesures contribuent uniquement à réduire le risque, mais elles ne constituent pas une mesure préventive contre les attaques DoS visant les services RAVPN.

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 des mesures de sécurisation pour réduire les risques d'impact de ces attaques :

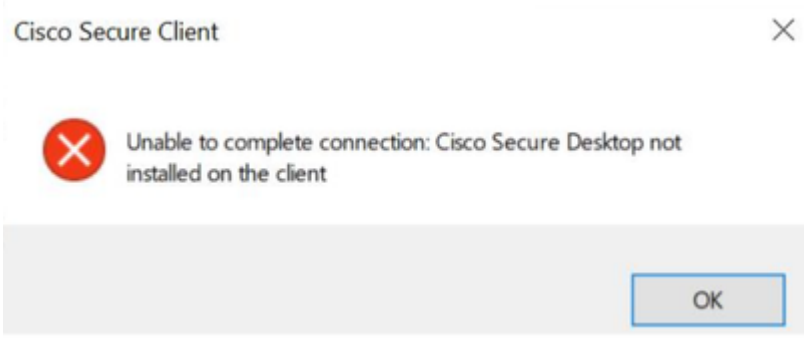
1. Désactivez l'authentification AAA dans les profils de connexion DefaultWEBVPN et DefaultRAGroup (étape par étape : ASA|FTD géré par FMC).
2. Désactivez Secure Firewall Posture (Hostscan) à partir des groupes DefaultWEBVPNGroup et DefaultRAGroup (étape par étape : ASA|FTD géré par FMC).
3. Désactivez 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 supplémentaire avec FTD géré via la gestion locale des pare-feu (FDM), contactez le TAC Cisco pour obtenir des conseils d'experts.

Pour plus de détails, référez-vous au Guide Implémenter des mesures de renforcement pour le client sécurisé AnyConnect VPN.

Comportements connexes

Les utilisateurs ne peuvent pas établir de connexions VPN avec Cisco Secure Client (AnyConnect) lorsque la position du pare-feu (HostScan) est activée sur Secure Firewall. Il peut rencontrer par intermittence un message d'erreur indiquant « Unable to complete connection. Cisco Secure Desktop n'est pas installé sur le client.



Ce comportement est une conséquence de l'exploitation réussie de la vulnérabilité CVE-2024-20481 décrite ci-après.

ID de bogue Cisco CSCwj45822 : Vulnérabilité de force de déni de service du VPN d'accès à distance Cisco ASA et FTD (CVE-2024-20481)

Cette vulnérabilité est due à l'épuisement des ressources dû aux attaques par pulvérisation de mots de passe, au cours desquelles les pirates envoient de nombreuses requêtes d'authentification VPN au périphérique cible. Une exploitation réussie peut entraîner un déni de service pour le service RAVPN. Un symptôme clé de cet exploit est lorsque les utilisateurs rencontrent par intermittence le message « Unable to complete connection ». Cisco Secure Desktop n'est pas installé sur le client. lorsqu'ils tentent d'établir une connexion RAVPN à l'aide de Cisco Secure Client.

Pour corriger cette vulnérabilité, il est nécessaire d'effectuer une mise à niveau vers les versions logicielles répertoriées dans l'avis de sécurité. En outre, il est recommandé d'activer les fonctions de détection des menaces pour le VPN d'accès à distance après la mise à niveau de votre pare-feu sécurisé vers ces versions afin de vous protéger contre les attaques DoS visant les services RAVPN.

Référez-vous à l'avis de sécurité Vulnérabilité de déni de service de force brute du VPN d'accès à distance Cisco ASA et FTD pour plus de détails.

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, contactez le TAC Cisco. 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.