Contenu

Introduction

Une source externe à Cisco a libéré un programme pour déchiffrer des mots de passe utilisateur (et d'autres mots de passe) dans des fichiers de configuration Cisco. Le programme ne déchiffrera pas des mots de passe définis avec la commande enable secret. Le souci inattendu que ce programme a entraîné parmi des clients de Cisco nous a menés à suspecter que beaucoup de clients comptent sur le cryptage de mot de passe de Cisco pour plus de sécurité qu'il avait été originalement conçu. Ce document explique le modèle de sécurité derrière le cryptage de mot de passe de Cisco, et les limites de sécurité de ce cryptage.

Remarque: Cisco recommande que tous les périphériques de Cisco IOS implémentent le modèle de Sécurité d'Authentification, autorisation et comptabilité (AAA). AAA peut utiliser des bases de données locales, RADIUS et TACACS+.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Mots de passe utilisateur

Des mots de passe utilisateur et la plupart des autres mots de passe (*pas* **enables secrets**) dans des fichiers de configuration Cisco IOS sont chiffrés utilisant un schéma qui est très faible par des normes cryptographiques modernes.

Bien que Cisco ne distribue pas un programme de déchiffrement, au moins deux programmes différents de déchiffrement pour des mots de passe de Cisco IOS sont à la disposition du public sur l'Internet ; la première diffusion publique d'un tel programme dont Cisco se rend compte avait lieu début 1995. Nous nous attendrions à ce que n'importe quel cryptographe amateur puisse créer un nouveau programme avec peu d'effort.

Le schéma utilisé par Cisco IOS pour des mots de passe utilisateur n'a été jamais destiné pour résister à une attaque déterminée et intelligente. La structure de chiffrement a été conçue d'éviter le vol de mot de passe par l'intermédiaire de piller ou de renifler simple. On ne l'a jamais destiné pour se protéger contre quelqu'un conduisant un effort de mot de passe-fissuration sur le fichier de configuration.

En raison de l'algorithme de chiffrement faible, il a toujours été la position de Cisco que les clients devraient traiter n'importe quel fichier de configuration contenant des mots de passe comme informations confidentielles de la même manière qu'ils traiteraient une liste de libellé de mots de passe.

enable secret et mot de passe d'enable

La commande de **mot de passe d'enable** devrait plus n'être utilisée. Utilisez la commande **enable secret** qui offre une meilleure sécurité. Le seul exemple dans lequel la commande de **mot de passe d'enable** pourrait être testée est quand le périphérique s'exécute dans un mode de démarrage qui ne prend en charge pas la **commande enable secret**.

Des enables secrets sont hachés utilisant l'algorithme de MD5. Dans la mesure où n'importe qui à Cisco sait, il est impossible de récupérer un enable secret basé sur le contenu d'un fichier de configuration (autre que par des attaques par dictionnaire évidentes).

Remarque: Ceci s'applique seulement aux mots de passe réglés avec l'**enable secret**, et *pas aux* mots de passe réglés avec le **mot de passe d'enable**. En effet, le point fort du cryptage utilisé est la seule différence important entre les deux commandes.

Quelle image de Cisco IOS prend en charge l'enable secret ?

Regardez votre image de démarrage utilisant la commande de **show version de** votre mode de fonctionnement normal (pleine image de Cisco IOS) de voir si l'image de démarrage prend en charge la **commande enable secret**. S'il fait, retirer le **mot de passe d'enable**. Si l'image de démarrage ne prend en charge pas l'**enable secret**, notez les mises en garde suivantes :

- L'établissement d'un mot de passe d'enable pourrait être inutile si vous avez la Sécurité physique de sorte que personne ne puisse recharger le périphérique à l'image de démarrage.
- Si quelqu'un a accès physique au périphérique, il peut facilement renverser la sécurité des périphériques sans devoir accéder à l'image de démarrage.
- Si vous placiez le **mot de passe d'enable aux** mêmes que l'**enable secret**, vous avez fait

l'attaque aussi encline d'**enable secret** que le **mot de passe d'enable**.
- Si vous placez le **mot de passe d'enable à une** valeur différente parce que l'image de démarrage ne prend en charge pas l'**enable secret**, vos administrateurs de routeur doivent se souvenir un nouveau mot de passe qui est utilisé rarement sur les ROM qui ne prennent en charge pas la **commande enable secret**. En ayant un mot de passe distinct d'enable, les administrateurs peuvent ne pas se souvenir le mot de passe quand ils forcent le temps d'arrêt pour une mise à niveau de logiciel, qui est la seule raison d'ouvrir une session au mode de démarrage.

D'autres mots de passe

Presque tous les mots de passe et d'autres chaînes d'authentification dans des fichiers de configuration Cisco IOS sont chiffrés utilisant le schéma faible et réversible utilisé pour des mots de passe utilisateur.

Pour déterminer quel schéma a été utilisé de chiffrer un mot de passe spécifique, vérifiez le chiffre précédant la chaîne chiffrée dans le fichier de configuration. Si ce chiffre est des 7, le mot de passe a été chiffré utilisant l'algorithme faible. Si le chiffre est des 5, le mot de passe a été haché utilisant l'algorithme plus fort de MD5.

Par exemple, dans la commande de configuration :

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

L'enable secret a été haché avec le MD5, tandis que dans la commande :

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

Le mot de passe a été chiffré utilisant l'algorithme réversible faible.

Fichiers de configuration

Quand vous envoyez les informations de configuration dans le courrier électronique, vous devriez assainir la configuration des mots de passe du type 7. Vous pouvez utiliser la commande de **show tech-support**, qui assainit les informations par défaut. La sortie de commande de **show tech-support** témoin est affichée ci-dessous.

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

En enregistrant vos fichiers de configuration sur un serveur de Protocole TFTP (Trivial File Transfer Protocol), changez les privilèges sur ce fichier quand il est non utilisable ou mis lui derrière un Pare-feu.

L'algorithme peut-il être changé ?

Cisco n'a aucun plan immédiat pour prendre en charge un algorithme de chiffrement plus fort pour des mots de passe utilisateur de Cisco IOS. Si Cisco décide d'introduire une telle caractéristique à l'avenir, cette caractéristique imposera certainement une charge administrative supplémentaire aux utilisateurs qui choisissent de tirer profit de elle.

Il n'est pas, dans le cas général, possible de commuter des mots de passe utilisateur plus d'à l'algorithme basé sur du Maryland utilisé pour des enables secrets, parce que le MD5 est des informations parasites à sens unique, et le mot de passe ne peut pas être récupéré des données

cryptées du tout. Afin de prendre en charge certains Protocoles d'authentification (notamment CHAP), l'accès des besoins de système au texte clair des mots de passe utilisateur, et doit donc les enregistrer utilisant un algorithme réversible.

Les questions de gestion des clés lui feraient une tâche non triviale de s'orienter vers un algorithme réversible plus fort, tel que le DES. Bien qu'il soit facile de modifier le Cisco IOS pour employer le DES pour chiffrer des mots de passe, il n'y aurait aucun avantage en matière de sécurité ce faisant, si tous les systèmes de Cisco IOS utilisaient la même clé DES. Si différentes clés étaient utilisées par des autres systèmes, une charge administrative serait introduite pour tous les administrateurs de réseau Cisco IOS, et la portabilité des fichiers de configuration entre les systèmes serait endommagée. La requête du client pour un cryptage réversible plus fort de mot de passe a été petite.

Informations connexes

- Procédures de récupération de mot de passe
- Guide Cisco pour renforcer les périphériques Cisco IOS
- Support technique - Cisco Systems