Comprendre le chiffrement de mot de passe Cisco IOS

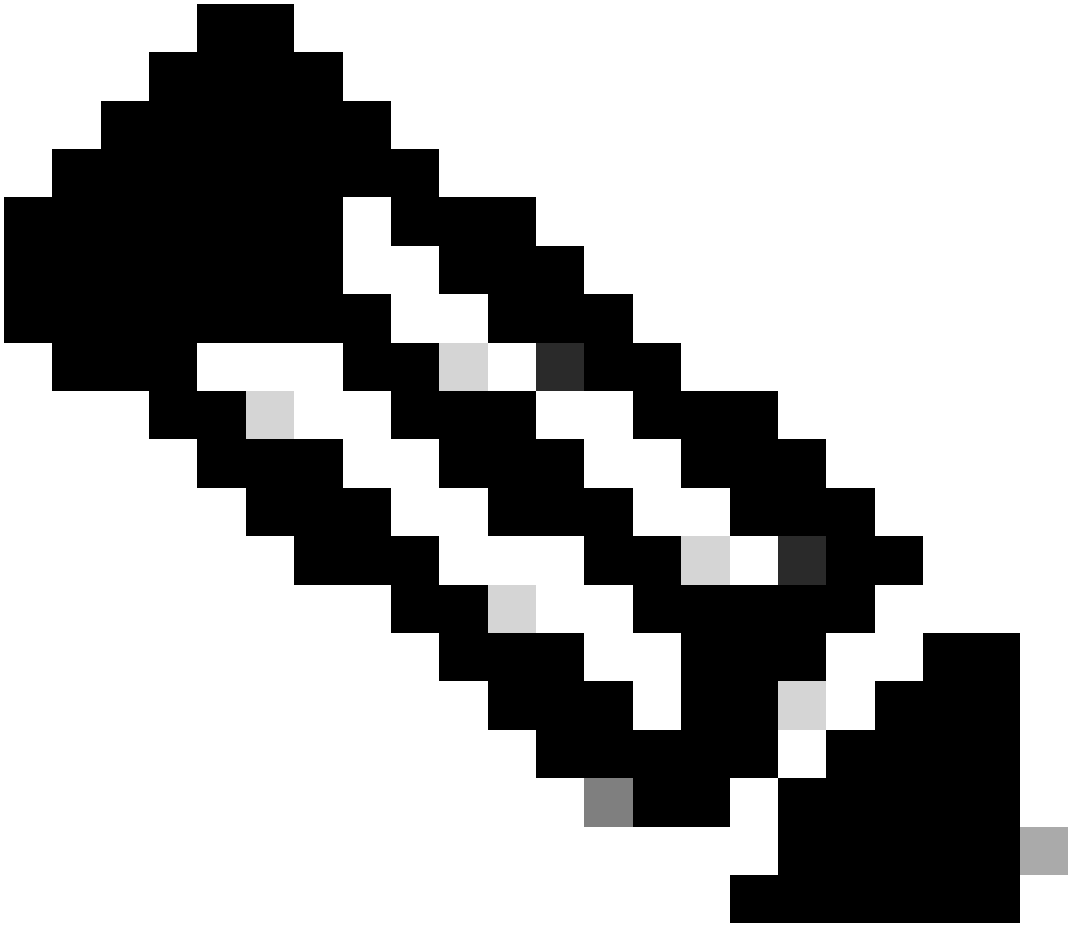
Table des matières

Introduction

Ce document décrit le modèle de sécurité derrière le chiffrement de mot de passe Cisco, et les limitations de sécurité de ce chiffrement.

Fond

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 déchiffre pas les mots de passe définis avec la **enable secret** commande. Les préoccupations inattendues que ce programme a suscitées chez les utilisateurs Cisco ont conduit à la suspicion que de nombreux utilisateurs dépendent du chiffrement de mot de passe Cisco pour plus de sécurité qu'il n'a été conçu pour fournir.



Remarque : Cisco recommande que tous les périphériques Cisco IOS® implémentent le modèle de sécurité AAA (Authentication, Authorization, and Accounting). AAA peut utiliser des bases de données locales, RADIUS et TACACS+.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Mots de passe des utilisateurs

Les mots de passe utilisateur, et la plupart des autres mots de passe (*pas* **enable secret**s) dans les fichiers de configuration Cisco IOS, sont chiffrés avec un schéma très faible selon les normes de chiffrement modernes.

Bien que Cisco ne distribue pas de programme de décryptage, au moins deux programmes de décryptage différents pour les mots de passe Cisco IOS sont accessibles au public sur Internet ; la première version publique d'un tel programme dont Cisco a connaissance remonte au début de 1995. Nous nous attendions à ce que tout cryptographe amateur parvienne à créer un nouveau programme, sans trop d’efforts.

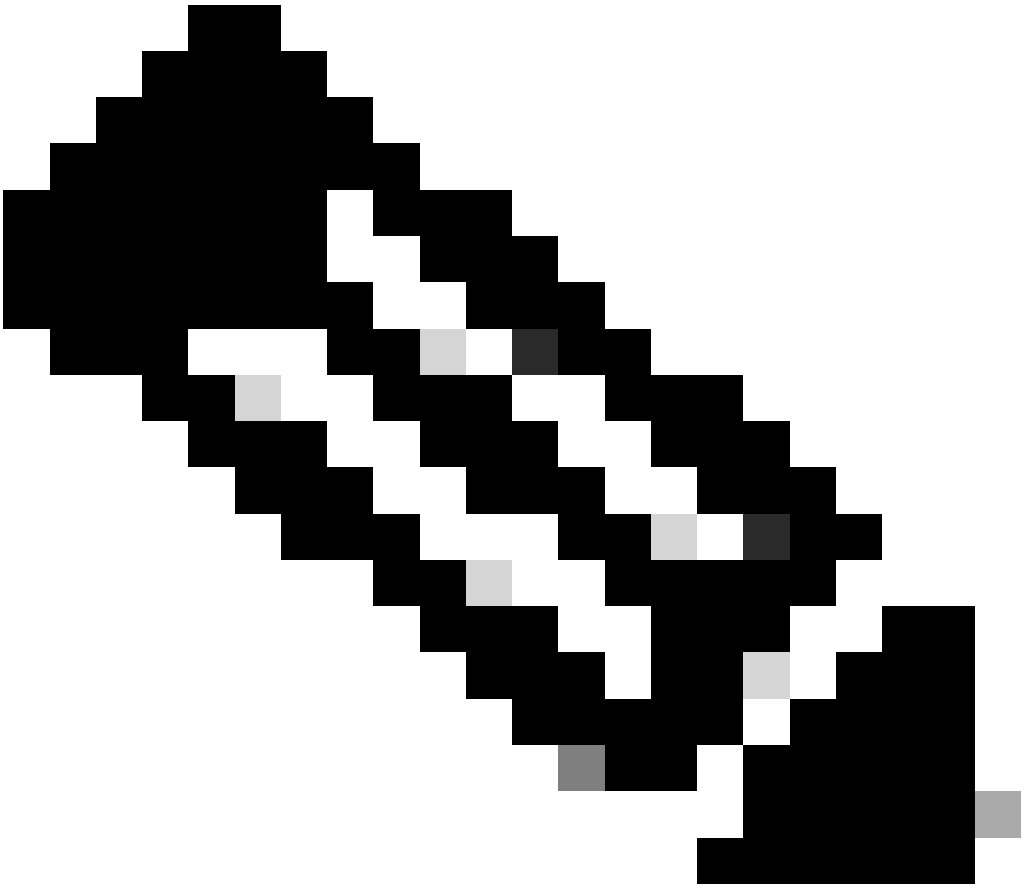
Le schéma qu’utilise Cisco IOS pour les mots de passe des utilisateurs n’a jamais été conçu pour résister à une attaque intelligente et déterminée. Le schéma de cryptage a été conçu pour éviter le vol de mots de passe par simple espionnage ou reniflement. Il n'a jamais été conçu pour se protéger contre une personne qui effectue une tentative de piratage de mot de passe sur le fichier de configuration.

En raison de la faiblesse de l'algorithme de chiffrement, Cisco a toujours considéré que les utilisateurs traitaient tout fichier de configuration contenant des mots de passe comme des informations sensibles, de la même manière qu'ils traiteraient une liste de mots de passe en texte clair.

Commandes enable secret et enable password

Il n'est plus recommandé d'utiliser cette enable password commande. Utilisez la commandeenable secret pour améliorer la sécurité. La seule instance dans laquelle la **enable password** commande peut être testée est lorsque le périphérique est dans un mode de démarrage qui ne prend pas en charge la enable secret commande.

Les secrets d'activation sont hachés avec l'algorithme MD5. À la connaissance de Cisco, il est impossible de récupérer une commande « enable secret » en fonction du contenu d’un fichier de configuration (hormis par des attaques évidentes par dictionnaire).



Remarque : ceci s'applique uniquement aux mots de passe définis avec enable secret, et non aux mots de passe définis avec **enable password**. En effet, la force du chiffrement utilisé est la seule différence notable entre les deux commandes.

Quels sont les supports d’images Cisco IOS qui activent le secret?

Examinez votre image de démarrage avec la **show version** commande de votre mode de fonctionnement normal (image complète de Cisco IOS) pour voir si l'image de démarrage prend en charge la **enable secret** commande. Si c'est le cas, supprimez le **enable password**. Si l'image de démarrage ne prend pas en charge **enable secret**, notez les avertissements suivants :

- L'utilisation d'un mot de passe enable peut être inutile si vous disposez d'une sécurité physique afin que personne ne puisse recharger le périphérique sur l'image de démarrage.

- Si une personne a un accès physique au périphérique, elle peut facilement contourner la sécurité du périphérique sans avoir besoin d'accéder à l'image de démarrage.

- Si vous définissez le sur **enable password** le même que le enable secret, vous avez rendu le enable secret aussi enclin à attaquer que le **enable password**.

    - Si vous définissez une valeur différente parce que l'image de démarrage ne prend pas **enable password** en charge **enable secret**, les administrateurs de votre routeur doivent se souvenir d'un nouveau mot de passe qui est rarement utilisé sur les mémoires ROM qui ne prennent pas en charge la **enable secret** commande. Avec un mot de passe enable distinct, les administrateurs doivent se souvenir du mot de passe lorsqu'ils forcent une interruption pour une mise à niveau logicielle, ce qui est la seule raison de se connecter au mode de démarrage.

Autres mots de passe

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

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

Par exemple, dans la commande de configuration :

```
<#root>
```

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

La commande « enable secret » a été hachée avec MD5, alors que dans la commande :

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

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

Fichiers de configuration

Lorsque vous envoyez des informations de configuration par e-mail, vérifiez la configuration à partir de mots de passe de type 7. Vous pouvez utiliser la commandeshow tech-support, qui vérifie les informations par défaut. L'exemple de sortie de **show tech-support** commande est présenté ici :

<#root>

```
...
 hostname routerA
 !
 aaa new-model
 aaa authentication login default local
 aaa authentication ppp default if-needed local
```

enable secret 5 <removed>

```
!


username jdoe password 7 <removed>
username headquarters password 7 <removed>
username hacker password 7 <removed>


...
```

Lorsque vous enregistrez vos fichiers de configuration sur un serveur TFTP (Trivial File Transfer Protocol), modifiez les privilèges de ce fichier lorsqu'il n'est pas utilisé ou placez-le derrière un pare-feu.

L’algorithme peut-il être modifié?

Cisco n’a aucun projet immédiat visant à prendre en charge un algorithme de chiffrement renforcé pour les mots de passe d’utilisateur Cisco IOS. Si Cisco décide d'introduire une telle fonctionnalité à l'avenir, celle-ci impose certainement une charge administrative supplémentaire aux utilisateurs qui choisissent d'en bénéficier.

Dans le cas général, il n'est pas possible de commuter les mots de passe utilisateur sur l'algorithme MD5 utilisé pour les secrets d'activation, car MD5 est un hachage unidirectionnel et le mot de passe ne peut pas être récupéré à partir des données chiffrées. Afin de prendre en charge certains protocoles d'authentification (notamment CHAP), le système a besoin d'accéder au texte clair des mots de passe utilisateur, et doit donc les stocker avec un algorithme réversible.

Les problèmes de gestion des clés rendraient difficile le passage à un algorithme réversible plus puissant, tel que Data Encryption Standard (DES). Bien qu’il soit facile de modifier Cisco IOS pour utiliser DES pour chiffrer les mots de passe, cette approche ne présente aucun avantage en termes de sécurité si tous les systèmes Cisco IOS utilisent la même clé DES. Si différentes clés étaient utilisées par les divers systèmes, une charge administrative serait alors imposée aux administrateurs réseau de Cisco IOS, et la portabilité des fichiers de configuration entre les systèmes serait endommagée. La demande des utilisateurs pour un chiffrement réversible renforcé des mots de passe a été faible.

Informations connexes

- **Procédures de récupération de mot de passe**
- **Guide Cisco pour renforcer les périphériques Cisco IOS**

- **Support technique - Cisco Systems**

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.