Entender os fatos de criptografia de senha do Cisco IOS

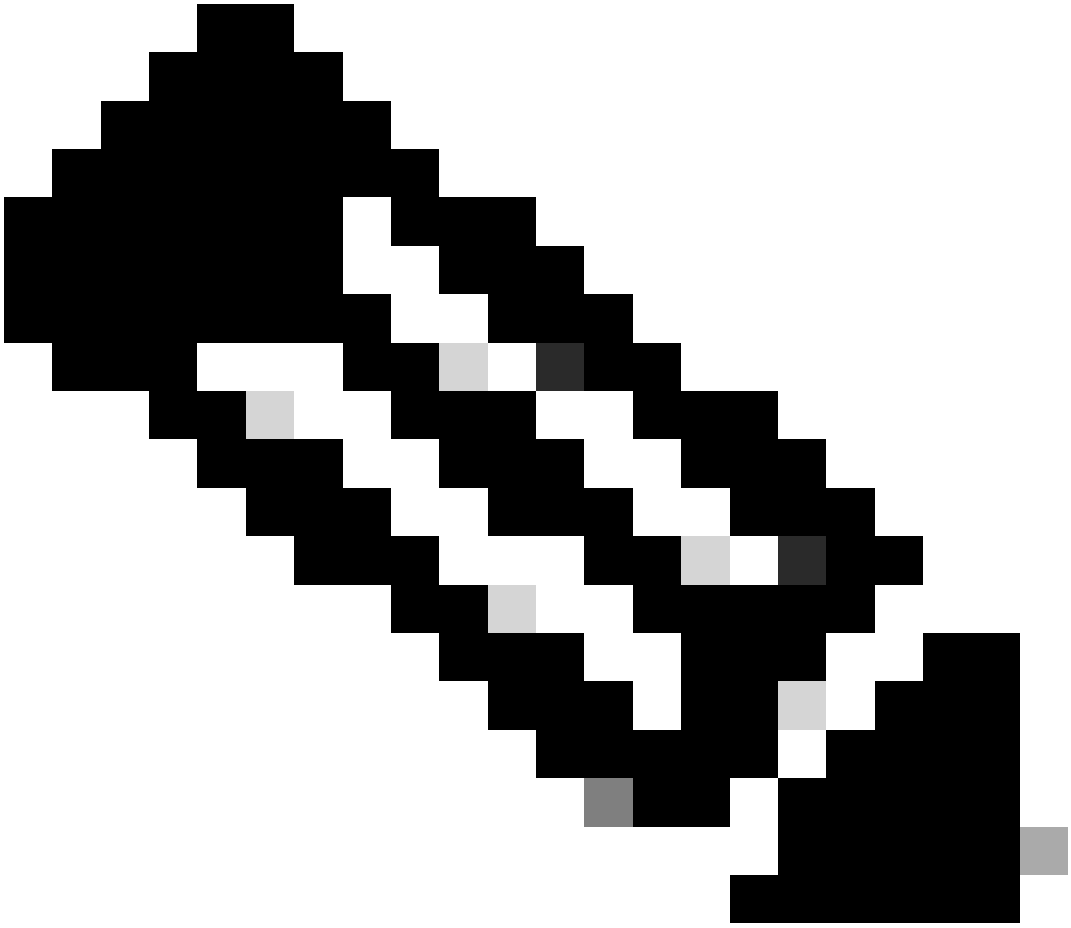
Contents

Introdução

Este documento descreve o modelo de segurança por trás da criptografia de senha da Cisco e as limitações de segurança dessa criptografia.

Background

Uma origem que não é da Cisco lançou um programa para decodificar senhas de usuário (e outras senhas) em arquivos de configuração da Cisco. O programa não descriptografa senhas definidas com o **enable secret** comando. A preocupação inesperada que o programa causou entre os usuários da Cisco levou à suspeita de que muitos usuários confiam na criptografia de senha da Cisco para obter mais segurança do que a projetada para oferecer.



Observação: a Cisco recomenda que todos os dispositivos Cisco IOS® implementem o modelo de segurança de autenticação, autorização e contabilização (AAA). AAA pode utilizar bancos de dados local, RADIUS e TACACS+.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Senhas de usuário

As senhas de usuário e a maioria das outras senhas (*não* **enable secret**s*) nos arquivos de configuração do Cisco IOS são criptografadas com um esquema muito fraco pelos padrões criptográficos modernos.*

Embora a Cisco não distribua um programa de descriptografia, pelo menos dois programas de descriptografia diferentes para senhas do Cisco IOS estão disponíveis para o público na Internet; a primeira versão pública de tal programa que a Cisco conhece foi no início de 1995. Esperamos que qualquer criptógrafo amador seja capaz de criar um novo programa com pouco esforço.

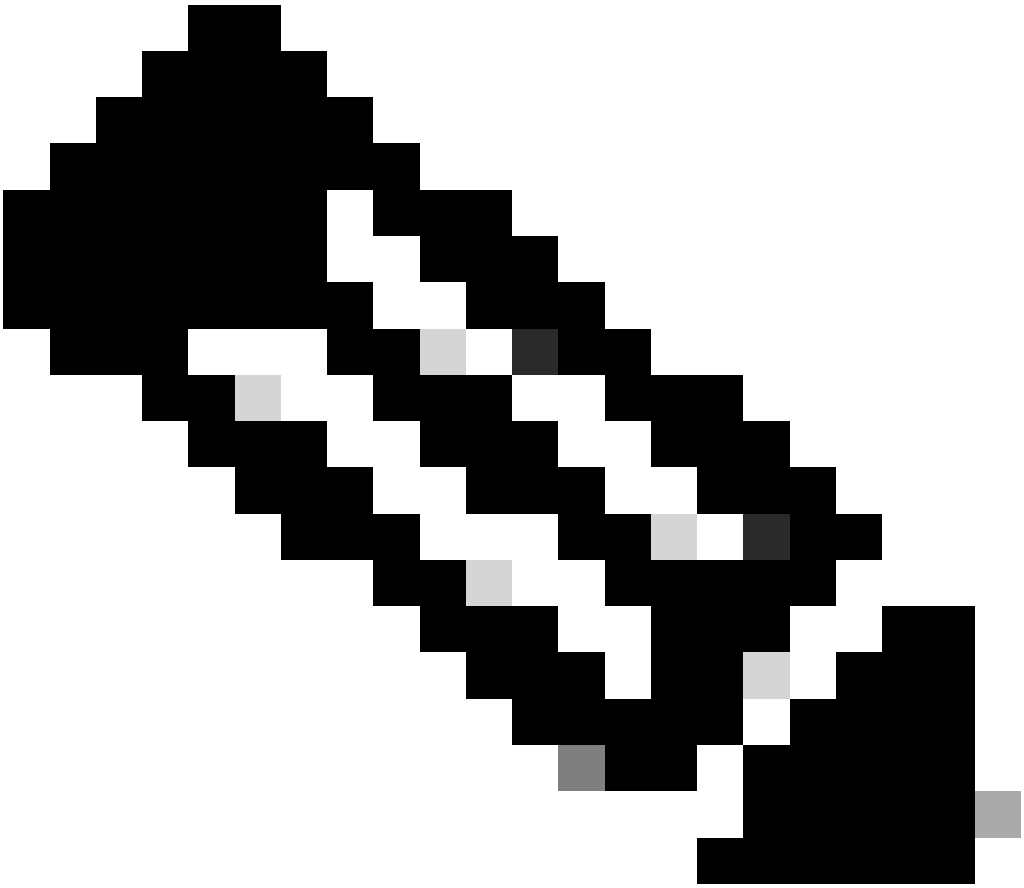
O esquema usado pelo Cisco IOS para senhas de usuário nunca foi projetado para resistir a um determinado ataque inteligente. O esquema de criptografia foi criado para evitar o roubo de senhas por simples espionagem ou farejamento. Ele nunca foi projetado para proteger contra alguém que realiza um esforço de decifração de senha no arquivo de configuração.

Devido ao algoritmo de criptografia fraco, sempre foi a posição da Cisco que os usuários tratam qualquer arquivo de configuração que contenha senhas como informações confidenciais, da mesma forma que tratariam uma lista de senhas em texto claro.

Os Comandos enable secret e enable password

O enable password comando não é mais recomendado para ser usado. Use o comandoenable secret para melhor segurança. A única instância em que o **enable password** comando pode ser testado é quando o dispositivo está em um modo de inicialização que não oferece suporte ao enable secret comando.

Os segredos de ativação são divididos em hash com o algoritmo MD5. Até onde se sabe na Cisco, é impossível recuperar um comando enable secret com base no conteúdo de um arquivo de configuração (além obviamente dos ataques de dicionários).



Observação: isso se aplica somente a senhas definidas com enable secret e não a senhas definidas com **enable password**. De fato, a força da criptografia usada é a única diferença significativa entre os dois comandos.

Quais suportes de imagem do Cisco IOS permitem segredo?

Examine sua imagem de inicialização com o **show version** comando do seu modo operacional normal (imagem completa do Cisco IOS) para ver se a imagem de inicialização suporta o **enable secret** comando. Se isso acontecer, remova o **enable password**. Se a imagem de inicialização não suportar **enable secret**, observe estes avisos:

- O uso de uma senha de ativação pode ser desnecessário se você tiver segurança física para que ninguém possa recarregar o dispositivo para a imagem de inicialização.

- Se alguém tiver acesso físico ao dispositivo, poderá subverter facilmente a segurança do dispositivo sem precisar acessar a imagem de inicialização.

- Se você definir **enable password** o como o mesmo que o enable secret, você terá feito o enable secret com tanta tendência a ataque quanto o **enable password**.

    - Se você definir **enable password** um valor diferente porque a imagem de inicialização não suporta **enable secret**, os administradores do roteador deverão lembrar de uma nova senha que é usada com pouca frequência em ROMs que não suportam o **enable secret** comando. Com uma senha de ativação separada, os administradores precisam lembrar a senha quando forçam um tempo de inatividade para uma atualização de software, que é o único motivo para fazer login no modo de inicialização.

Outras senhas

Quase todas as senhas e outras cadeias de caracteres de autenticação nos arquivos de configuração do Cisco IOS são criptografadas com o esquema fraco e reversível usado para as senhas de usuário.

Para determinar qual esquema foi usado para criptografar uma senha específica, verifique o dígito antes da cadeia de caracteres criptografada no arquivo de configuração. Se esse dígito for 7, a senha foi criptografada com o algoritmo fraco. Se o dígito for 5, a senha foi misturada com o algoritmo MD5 mais forte.

Por exemplo, no comando de configuração:"

```
<#root>
```

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

O segredo habilitado recebeu o código hash MD5, enquanto no comando:

```
<#root>
```

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

A senha foi criptografada com o algoritmo reversível fraco.

Arquivos de configuração

Quando você envia informações de configuração em e-mail, limpe a configuração das senhas tipo 7. Você pode usar o comandoshow tech-support, que limpa as informações por padrão. Um exemplo de saída de **show tech-support** comando é mostrado aqui:

```
<#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>
```

...

Quando você salva os arquivos de configuração em um servidor TFTP, altere os privilégios desse arquivo quando ele não estiver em uso ou coloque-o atrás de um firewall.

O algoritmo pode ser alterado?

A Cisco não tem planos imediatos para suportar um algoritmo de criptografia mais forte para as senhas de usuário do Cisco IOS. Se a Cisco decidir introduzir esse recurso no futuro, ele definitivamente impõe uma carga administrativa adicional aos usuários que escolherem aproveitá-lo.

Não é possível, no caso geral, trocar as senhas de usuário para o algoritmo baseado em MD5 usado para habilitar segredos, porque o MD5 é um hash unidirecional e a senha não pode ser recuperada dos dados criptografados. Para suportar certos protocolos de autenticação (nomeadamente o CHAP), o sistema precisa de acesso ao texto claro das senhas dos usuários e, portanto, deve armazená-las com um algoritmo reversível.

Problemas de gerenciamento de chaves tornariam uma tarefa não trivial mudar para um algoritmo reversível mais forte, como o Data Encryption Standard (DES). Embora fosse fácil modificar o Cisco IOS para usar o DES para criptografar senhas, não haveria nenhuma vantagem de segurança nessa abordagem, se todos os sistemas Cisco IOS usassem a mesma chave DES. Se fossem usadas chaves diferentes por sistemas diferentes, seria introduzida uma sobrecarga administrativa para todos os administradores de rede Cisco IOS e a portabilidade dos arquivos de configuração entre os sistemas seria danificada. A demanda do usuário por uma criptografia de senha reversível mais forte foi pequena.

Informações Relacionadas

- **Procedimentos de recuperação de senhas**
- **Guia da Cisco para fortalecer dispositivos IOS Cisco**

- **Suporte Técnico - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.