Comprender los hechos del cifrado de contraseña de Cisco IOS

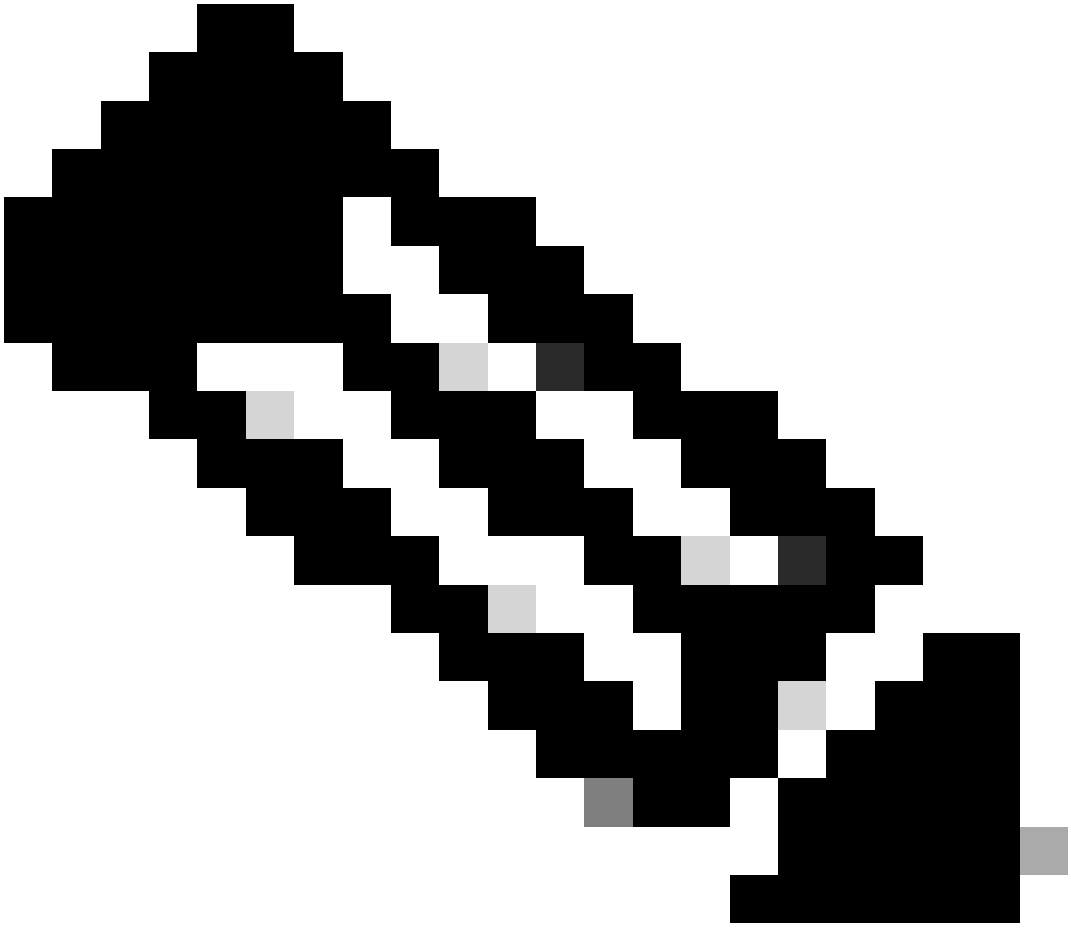
Contenido

Introducción

Este documento describe el modelo de seguridad detrás del cifrado de contraseña de Cisco y las limitaciones de seguridad de ese cifrado.

Background

Una fuente que no es Cisco ha lanzado un programa para descifrar contraseñas de usuarios (y otras contraseñas) en archivos de configuración Cisco. El programa no descifra las contraseñas establecidas con el **enable secret** comando. La inesperada preocupación que el programa causó entre los usuarios de Cisco ha llevado a la sospecha de que muchos usuarios confían en el cifrado de contraseña de Cisco para más seguridad de la que se diseñó para proporcionar.



Nota: Cisco recomienda que todos los dispositivos Cisco IOS® implementen el modelo de seguridad de autenticación, autorización y contabilidad (AAA). AAA puede emplear bases de datos locales, RADIUS y TACACS+.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Contraseñas de usuarios

Las contraseñas de usuario y la mayoría de las otras contraseñas (*no* **enable secret**s) en los archivos de configuración del IOS de Cisco, se cifran con un esquema que es muy débil según los estándares criptográficos modernos.

Aunque Cisco no distribuye un programa de descifrado, hay al menos dos programas de descifrado diferentes para las contraseñas de Cisco IOS disponibles para el público en Internet; la primera versión pública de dicho programa, de la que Cisco es consciente, fue a principios de 1995. Esperamos que cualquier criptógrafo aficionado sea capaz de crear un nuevo programa con poco esfuerzo.

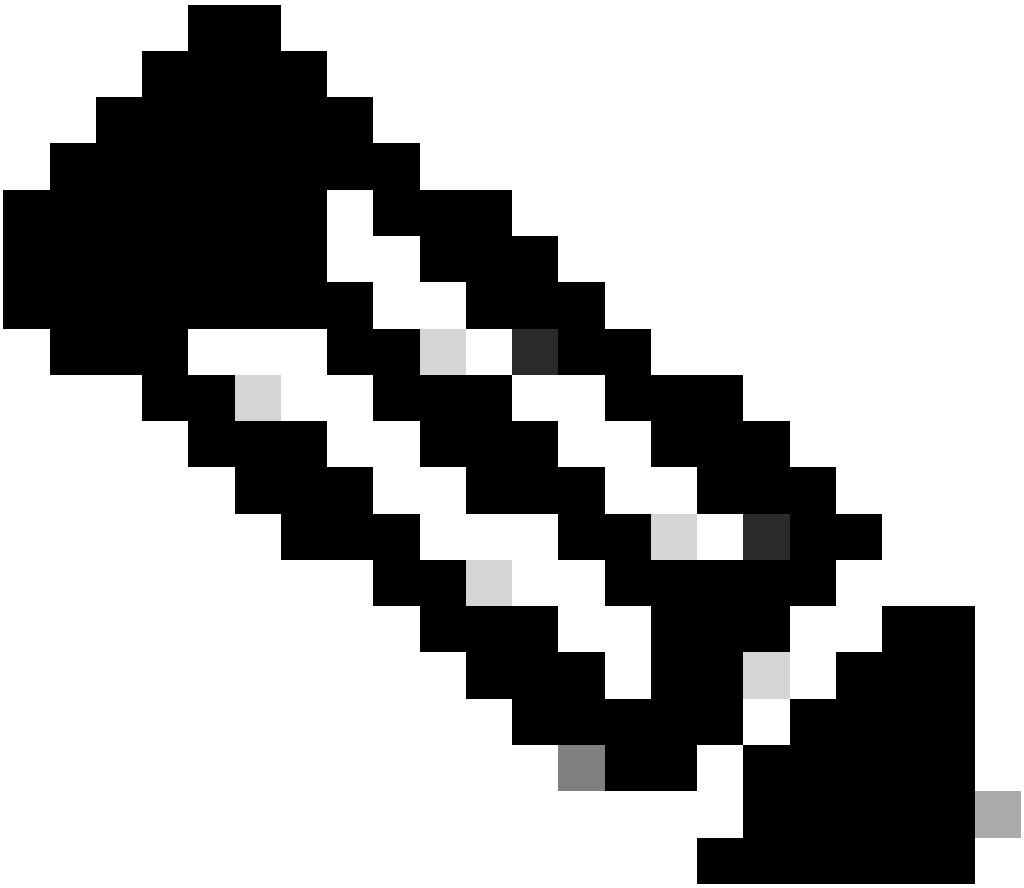
El esquema utilizado por Cisco IOS para las contraseñas de usuario nunca fue pensado para resistir un ataque inteligente determinado. El esquema de cifrado se ha diseñado para evitar el robo de contraseñas mediante la detección o el rastreo sencillos. Nunca fue pensado para proteger contra alguien que lleva a cabo un esfuerzo de descifrado de contraseñas en el archivo de configuración.

Debido al algoritmo de cifrado débil, siempre ha sido la posición de Cisco que los usuarios traten cualquier archivo de configuración que contenga contraseñas como información confidencial, de la misma manera que tratarían una lista de texto sin cifrar de contraseñas.

Los comandos enable secret y enable password

Ya no se recomienda utilizar el enable password comando. Utilice el enable secret comando para una mayor seguridad. La única instancia en la que se puede probar el **enable password** comando es cuando el dispositivo está en un modo de arranque que no admite el enable secret comando.

Los secretos de habilitación se codifican con el algoritmo MD5. Según la información que tenemos en Cisco, es imposible recuperar un habilitar secreto basado en los contenidos de un archivo de configuración (a no ser por medio de ataques obvios al diccionario).



Nota: Esto sólo se aplica a las contraseñas establecidas con enable secret, y no a las contraseñas establecidas con **enable password**. De hecho, la fuerza de la encriptación utilizada es la única diferencia significativa entre los dos comandos.

¿Qué imagen de Cisco IOS admite enable secret?

Observe la imagen de inicio con el **show version** comando del modo de funcionamiento normal (imagen completa de Cisco IOS) para ver si la imagen de inicio admite el **enable secret** comando. Si es así, desmonte el **enable password**. Si la imagen de arranque no es compatible **enable secret**, tenga en cuenta las siguientes advertencias:

- El uso de una contraseña de habilitación puede ser innecesario si tiene seguridad física para que nadie pueda recargar el dispositivo en la imagen de inicio.

- Si alguien tiene acceso físico al dispositivo, puede subvertir fácilmente la seguridad del dispositivo sin necesidad de acceder a la imagen de inicio.

- Si establece el en **enable password** el mismo que el enable secret, ha hecho que el enable secret sea tan propenso a ataques como el **enable password**.

    - Si establece un valor diferente debido **enable password** a que la imagen de inicio no es compatible **enable secret**, los administradores del router deben recordar una nueva contraseña que se utiliza con poca frecuencia en las ROM que no admiten el **enable secret** comando. Con una contraseña de activación independiente, los administradores deben recordar la contraseña cuando fuerzan un tiempo de inactividad para una actualización de software, que es la única razón para iniciar sesión en el modo de arranque.

Otras contraseñas

Casi todas las contraseñas y otras cadenas de autenticación de los archivos de configuración del IOS de Cisco se cifran con el esquema débil y reversible utilizado para las contraseñas de usuario.

Para determinar qué esquema se ha utilizado para cifrar una contraseña específica, compruebe el dígito que precede a la cadena cifrada en el archivo de configuración. Si ese dígito es un 7, la contraseña se ha cifrado con el algoritmo débil. Si el dígito es un 5, la contraseña se ha troceado con el algoritmo MD5 más fuerte.

Por ejemplo, en el comando de configuración:

```
<#root>
```

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

Se ha generado enable secret con MD5, mientras que en el comando:

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

La contraseña se ha cifrado con el algoritmo reversible débil.

Archivos de configuración

Cuando envíe información de configuración por correo electrónico, limpie la configuración de las contraseñas de tipo 7. Puede utilizar el show tech-support comando, que sanea la información de forma predeterminada. Aquí se muestra un ejemplo de resultado del **show tech-support** comando:

<#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>


...
```

Cuando guarde los archivos de configuración en un servidor TFTP (protocolo trivial de transferencia de archivos), cambie los privilegios de ese archivo cuando no esté en uso o colóquelo detrás de un firewall.

¿Se puede cambiar el algoritmo?

Cisco no tiene planes inmediatos para admitir un algoritmo de cifrado más fiable para las contraseñas de usuario de Cisco IOS. Si Cisco decide introducir una función de este tipo en el futuro, esta supone definitivamente una carga administrativa adicional para los usuarios que decidan aprovecharla.

En el caso general, no es posible cambiar las contraseñas de usuario al algoritmo basado en MD5 utilizado para habilitar secretos, porque MD5 es un hash unidireccional y la contraseña no se puede recuperar de los datos cifrados. Para admitir ciertos protocolos de autenticación (en particular CHAP), el sistema necesita acceder al texto sin cifrar de las contraseñas de usuario y, por lo tanto, debe almacenarlas con un algoritmo reversible.

Los problemas de administración de claves harían que sea una tarea no trivial cambiar a un algoritmo reversible más fuerte, como el Estándar de cifrado de datos (DES). Aunque sería fácil modificar Cisco IOS para utilizar DES para cifrar contraseñas, no habría ninguna ventaja de seguridad en este enfoque si todos los sistemas Cisco IOS utilizaran la misma clave DES. Si distintos sistemas utilizaran claves distintas, se introduciría una carga administrativa para todos los administradores de red y se dañaría la capacidad de transferencia de archivos de configuración entre los sistemas. La demanda por parte de los usuarios de un cifrado de contraseñas reversible más fiable ha sido pequeña.

Información Relacionada

- **Procedimientos para Recuperación de Contraseñas**
- **Guía de Cisco para fortalecer los dispositivos Cisco IOS**

- **Soporte Técnico - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).