Informazioni sui fatti relativi alla crittografia della password Cisco IOS

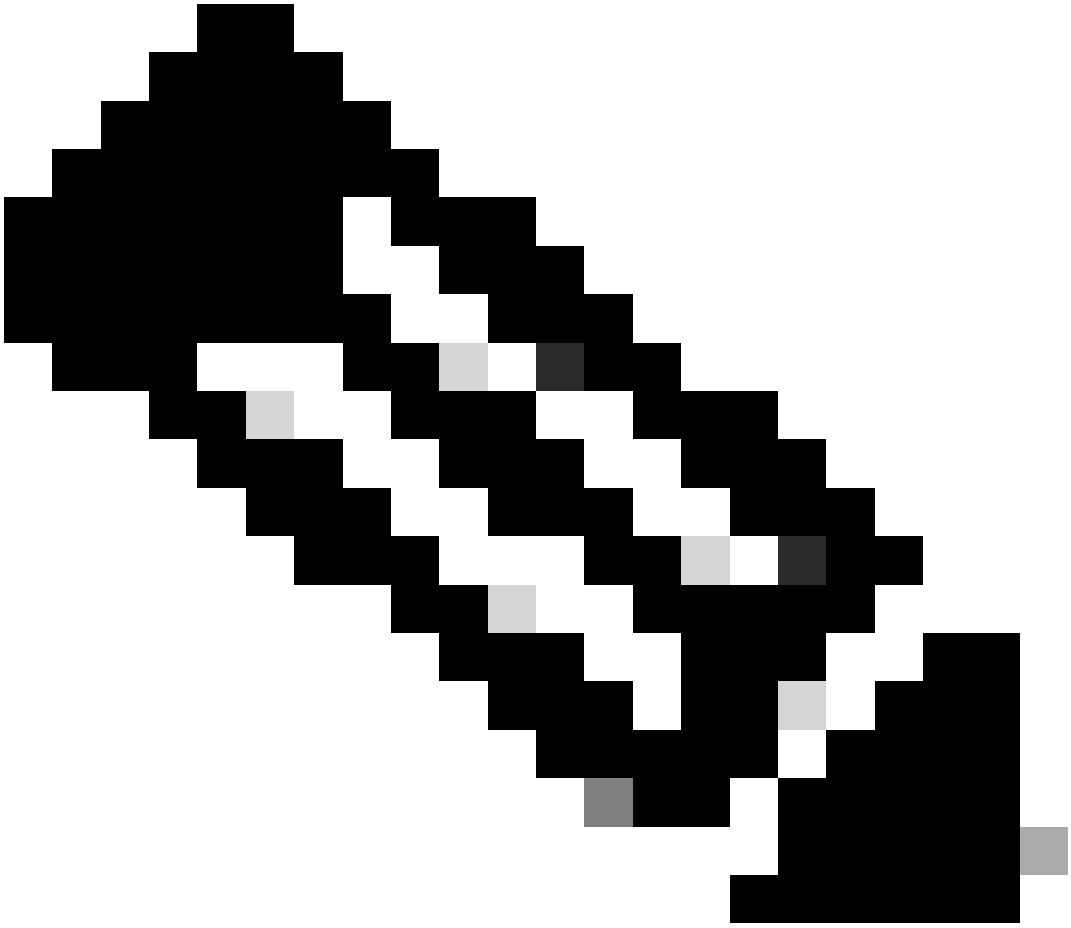
Sommario

Introduzione

Questo documento descrive il modello di sicurezza alla base della crittografia della password Cisco e i limiti di sicurezza di tale crittografia.

Introduzione

Un programma realizzato da una fonte esterna a Cisco permette di decriptare le password degli utenti (e altre password) nei file di configurazione Cisco. Il programma non decrittografa le password impostate con il **enable secret** comando. La preoccupazione inaspettata che il programma abbia causato tra gli utenti Cisco ha fatto nascere il sospetto che molti di essi si affidino alla crittografia della password Cisco per una sicurezza maggiore di quella per cui è stata progettata.



Nota: Cisco consiglia a tutti i dispositivi Cisco IOS® di implementare il modello di sicurezza autenticazione, autorizzazione e accounting (AAA). AAA può utilizzare database locali, RADIUS e TACACS+.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Password utente

Le password degli utenti e la maggior parte delle altre password (*non* **enable secret**s) nei file di configurazione di Cisco IOS sono crittografate con uno schema molto debole rispetto ai moderni standard di crittografia.

Sebbene Cisco non distribuisca un programma di decrittografia, almeno due diversi programmi di decrittografia per le password Cisco IOS sono disponibili al pubblico su Internet; la prima versione pubblica di un programma di questo tipo, di cui Cisco è a conoscenza, è stata rilasciata all'inizio del 1995. Ci aspetteremmo che qualsiasi crittografo dilettante sia in grado di creare un nuovo programma con poco sforzo.

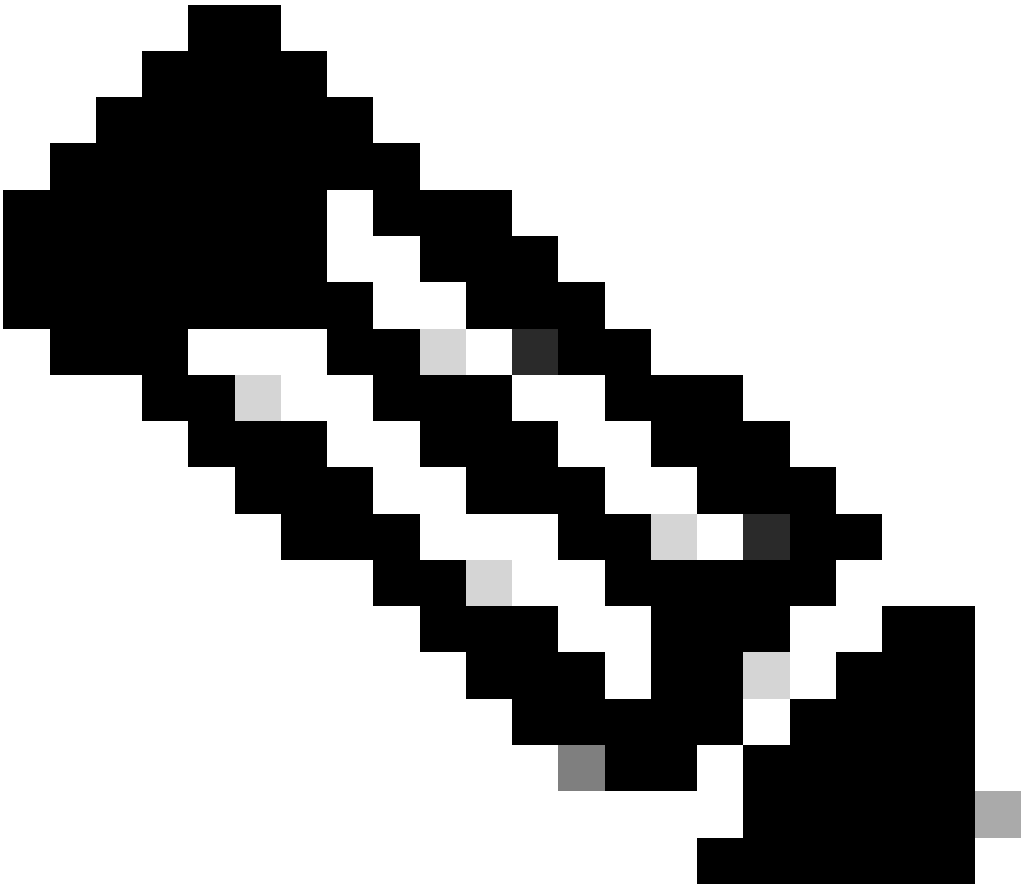
Lo schema usato da Cisco IOS per le password degli utenti non è mai stato pensato per resistere ad un attacco determinato e intelligente. Lo schema di crittografia è stato progettato per evitare il furto della password tramite semplici operazioni di snooping o sniffing. Non è mai stato progettato per proteggere il file di configurazione da utenti che tentano di intercettare le password.

A causa dell'algoritmo di crittografia vulnerabile, è sempre stato Cisco che gli utenti trattassero i file di configurazione che contengono password come informazioni riservate, allo stesso modo in cui gestirebbero un elenco di password in formato testo non crittografato.

Comandi enable secret e enable password

Si consiglia di non utilizzare più il enable password comando. Utilizzare il comandoenable secret per una maggiore sicurezza. L'unica istanza in cui è possibile testare il **enable password** comando è quando il dispositivo si trova in una modalità di avvio che non supporta il enable secret comando.

L'hash dei segreti di abilitazione viene eseguito con l'algoritmo MD5. A quanto ne sanno tutti in Cisco, è impossibile recuperare un segreto di abilitazione in base al contenuto di un file di configurazione (a parte ovvi attacchi da dizionario).



Nota: questo vale solo per le password impostate con enable secret e non per le password impostate con **enable password**. Infatti, la forza della crittografia utilizzata è l'unica differenza significativa tra i due comandi.

Quale immagine Cisco IOS supporta l'abilitazione del segreto?

Controllare l'immagine di avvio con il **show version** comando della modalità operativa normale (immagine Cisco IOS completa) per verificare se l'immagine di avvio supporta il **enable secret** comando. In caso affermativo, rimuovere il **enable password**file. Se l'immagine d'avvio non supporta **enable secret**, tenere presente le seguenti avvertenze:

- L'utilizzo di una password di abilitazione può non essere necessario se si dispone della protezione fisica in modo che nessuno possa ricaricare il dispositivo sull'immagine di avvio.

- Se qualcuno ha accesso fisico al dispositivo, può facilmente sovvertire la sicurezza del dispositivo senza dover accedere all'immagine d'avvio.

- Se si imposta il **enable password** su uguale a enable secret, si è reso il enable secret come incline ad attaccare come il **enable password**.

    - Se si imposta **enable password** un valore diverso perché l'immagine di avvio non supporta **enable secret**, gli amministratori del router devono ricordare una nuova password che viene utilizzata raramente nelle ROM che non supportano il **enable secret** comando. Con una password di abilitazione separata, gli amministratori devono ricordare la password quando forzano un downtime per un aggiornamento software, che è l'unico motivo per accedere alla modalità di avvio.

Altre password

Quasi tutte le password e le altre stringhe di autenticazione nei file di configurazione di Cisco IOS vengono crittografate con lo schema debole e reversibile usato per le password degli utenti.

Per determinare lo schema utilizzato per crittografare una password specifica, controllare la cifra prima della stringa crittografata nel file di configurazione. Se la cifra è 7, la password è stata crittografata con l'algoritmo di protezione vulnerabile. Se la cifra è un 5, la password è stata sottoposta a hashing con l'algoritmo MD5 più avanzato.

Ad esempio, nel comando configuration:

```
<#root>
```

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

Il segreto enable è stato sottoposto a hashing con MD5, mentre nel comando:

```
<#root>
```

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

La password è stata crittografata con l'algoritmo vulnerabile e reversibile.

File di configurazione

Quando si inviano informazioni di configurazione tramite posta elettronica, eliminare la configurazione dalle password di tipo 7. È possibile utilizzare il comandoshow tech-support che, per impostazione predefinita, elimina le informazioni. Di seguito è riportato un esempio di output 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>
```

```
...
```

Quando si salvano i file di configurazione su un server TFTP (Trivial File Transfer Protocol), modificare i privilegi su tale file quando non è in uso o posizionarlo dietro un firewall.

È Possibile Modificare L'Algoritmo?

Cisco non prevede di supportare immediatamente un algoritmo di crittografia più avanzato per le password degli utenti Cisco IOS. Se Cisco decide di introdurre una funzionalità di questo tipo in futuro, la funzionalità in questione imporrà sicuramente un ulteriore onere amministrativo agli utenti che scelgono di sfruttarla.

In generale, non è possibile passare le password utente all'algoritmo basato su MD5 utilizzato per abilitare i segreti, in quanto MD5 è un hash unidirezionale e la password non può essere recuperata dai dati crittografati. Per supportare alcuni protocolli di autenticazione (in particolare la protezione CHAP), il sistema deve accedere al testo non crittografato delle password utente, che devono quindi essere memorizzate con un algoritmo reversibile.

I problemi di gestione delle chiavi renderebbero non banale il passaggio a un algoritmo reversibile più avanzato, ad esempio il DES (Data Encryption Standard). Sebbene sia facile modificare Cisco IOS in modo che utilizzi DES per crittografare le password, questo approccio non offre vantaggi in termini di sicurezza se tutti i sistemi Cisco IOS utilizzassero la stessa chiave DES. Se i diversi sistemi utilizzassero chiavi diverse, verrebbe introdotto un onere amministrativo per tutti gli amministratori di rete Cisco IOS e la portabilità dei file di configurazione tra i sistemi ne risulterebbe danneggiata. La richiesta da parte degli utenti di una crittografia più avanzata e reversibile delle password è stata ridotta.

Informazioni correlate

- **Procedure di recupero della password**
- **Guida Cisco per fortificare i dispositivi Cisco IOS**

- **Supporto tecnico – Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).