Feiten over Cisco IOS-wachtwoordversleuteling

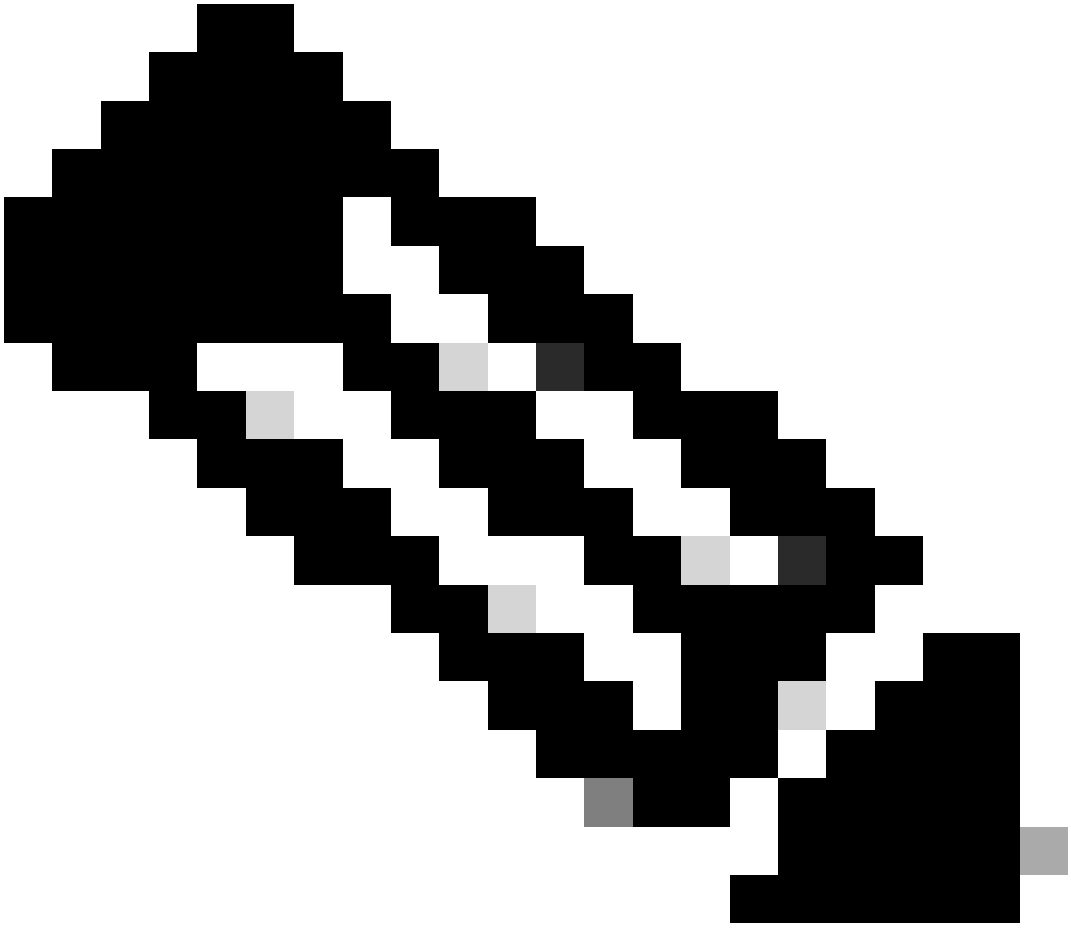
Inhoud

Inleiding

Dit document beschrijft het veiligheidsmodel achter de wachtwoordencryptie van Cisco, en de veiligheidsbeperkingen van die encryptie.

Achtergrond

Een niet-Cisco-bron heeft een programma ontwikkeld om gebruikerswachtwoorden (en andere wachtwoorden) te ontsleutelen in Cisco-configuratiebestanden. Het programma decrypteert geen wachtwoorden die met de **enable secret** opdracht zijn ingesteld. De onverwachte zorg dat het programma dat onder Cisco-gebruikers wordt veroorzaakt, heeft geleid tot het vermoeden dat veel gebruikers voor meer beveiliging vertrouwen op Cisco-wachtwoordcodering dan waarvoor het is ontworpen.



Opmerking: Cisco raadt aan dat alle Cisco IOS®-apparaten het verificatiemodel, autorisatie en accounting (AAA) implementeren. AAA kan lokale, RADIUS- en TACACS+-databases gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Gebruikerswachtwoorden

Gebruikerswachtwoorden en de meeste andere wachtwoorden (*niet* **enable secret**s) in Cisco IOS-configuratiebestanden worden versleuteld met een schema dat volgens moderne cryptografische normen zeer zwak is.

Hoewel Cisco geen decryptie programma distribueert, zijn er ten minste twee verschillende decryptie programma's voor Cisco IOS wachtwoorden beschikbaar voor het publiek op het internet; de eerste publieke release van een dergelijk programma waarvan Cisco zich bewust is, was begin 1995. We zouden verwachten dat elke amateur cryptograaf in staat is om een nieuw programma te creëren met weinig moeite.

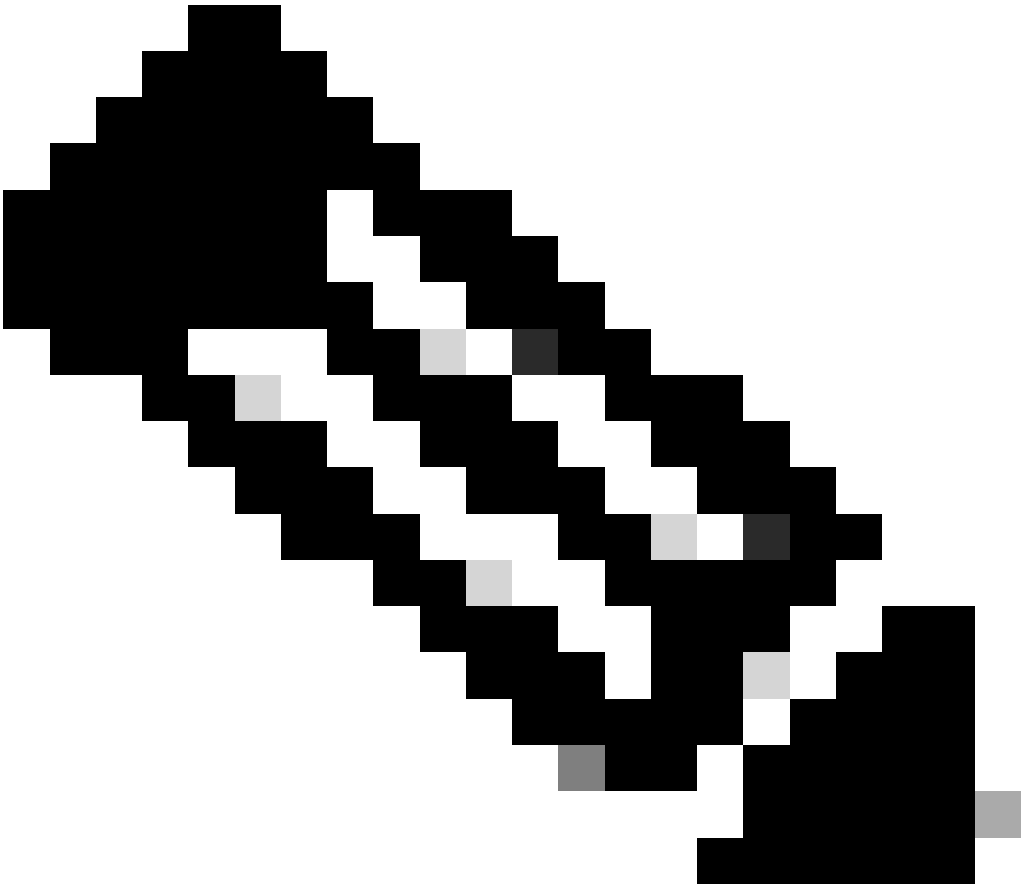
De regeling die door Cisco IOS wordt gebruikt voor gebruikerswachtwoorden is nooit bedoeld om weerstand te bieden aan een bepaalde, intelligente aanval. De coderingsmethode is ontworpen om wachtwoorddiefstal te voorkomen door eenvoudig snuffelen of snuiven. Het was nooit bedoeld om te beschermen tegen iemand die een wachtwoord-krakende inspanning op het configuratiebestand voert.

Wegens het zwakke encryptie-algoritme, is het altijd het standpunt van Cisco geweest dat de gebruikers om het even welk configuratiebestand behandelen dat wachtwoorden als gevoelige informatie bevat, de zelfde manier zij een duidelijke tekstlijst van wachtwoorden zouden behandelen.

Schakel geheime opdrachten in en schakel wachtwoordopdrachten in

De enable password opdracht wordt niet meer aanbevolen. Gebruik de opdracht voorenable secret een betere beveiliging. De enige instantie waarin de **enable password** opdracht kan worden getest is wanneer het apparaat zich in een opstartmodus bevindt die de opdracht niet ondersteuntenable secret.

Laat geheimen toe worden gehakt met het MD5 algoritme. Voor zover iedereen bij Cisco weet, is het onmogelijk om te herstellen en geheim toe te laten op basis van de inhoud van een configuratiebestand (anders dan door duidelijke woordenboekaanvallen).



Opmerking: dit is alleen van toepassing op wachtwoorden die zijn ingesteld met enable secret, en niet op wachtwoorden die zijn ingesteld met **enable password**. Sterker nog, de sterkte van de gebruikte encryptie is het enige significante verschil tussen de twee commando's.

Welke ondersteuning voor Cisco IOS-afbeeldingen maakt geheim mogelijk?

Bekijk uw opstartbeeld met de **show version** opdracht vanuit uw normale bedrijfsmodus (Full Cisco IOS-afbeelding) om te zien of het opstartbeeld de **enable secret** opdracht ondersteunt. Als dit het geval is, verwijdert u de **enable password**rest. Als het opstartbeeld niet wordt ondersteund, **enable secret**let dan op deze voorbehouden:

- Het gebruik van een inschakelen wachtwoord kan overbodig zijn als je fysieke beveiliging hebt, zodat niemand het apparaat kan herladen naar het opstartbeeld.

- Als iemand fysieke toegang tot het apparaat heeft, kunnen zij gemakkelijk de apparatenveiligheid omkeren zonder een behoefte om tot het laarsbeeld toegang te hebben.

- Als u de **enable password** aan het zelfde als het enable secret plaatst, hebt u enable secretzo voor de aanval als **enable password**vatbaar gemaakt.

    - Als u **enable password** aan een andere waarde plaatst omdat het laarsbeeld niet steunt **enable secret**, moeten uw routerbeheerders een nieuw wachtwoord herinneren dat niet vaak op ROMs wordt gebruikt die niet het **enable secret** bevel steunen. Met een apart inschakelen wachtwoord moeten beheerders het wachtwoord onthouden wanneer ze een downtime forceren voor een software-upgrade, wat de enige reden is om in te loggen op de opstartmodus.

Andere wachtwoorden

Bijna alle wachtwoorden en andere verificatietekeningen in Cisco IOS-configuratiebestanden zijn versleuteld met de zwakke, omkeerbare regeling die voor gebruikerswachtwoorden wordt gebruikt.

Om te bepalen welke regeling is gebruikt om een specifiek wachtwoord te versleutelen, controleert u het cijfer voor de versleutelde tekenreeks in het configuratiebestand. Als dat cijfer een 7 is, is het wachtwoord versleuteld met het zwakke algoritme. Als het cijfer een 5 is, is het wachtwoord gehakt met het sterkere MD5 algoritme.

In de configuratieopdracht bijvoorbeeld:

```
<#root>
```

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

Laat geheim toe is gehakt met MD5, terwijl in het bevel:

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

Het wachtwoord is versleuteld met het zwakke omkeerbare algoritme.

Configuratiebestanden

Wanneer u configuratie-informatie in e-mail verzendt, reinigt u de configuratie van wachtwoorden van type 7. U kunt de opdracht gebruikenshow tech-support, die de informatie standaard reinigt. Hier wordt voorbeeldopdrachtoutput **show tech-support** getoond:

<#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>


...
```

Wanneer u uw configuratiebestanden opslaat op een TFTP-server (Trivial File Transfer Protocol), wijzigt u de rechten van dat bestand wanneer het niet in gebruik is of plaatst u het achter een firewall.

Kan het algoritme worden gewijzigd?

Cisco heeft geen onmiddellijke plannen om een sterker encryptie-algoritme voor Cisco IOS-gebruikerswachtwoorden te ondersteunen. Als Cisco beslist zo'n functie in de toekomst te introduceren, legt deze zeker een extra administratieve last op aan gebruikers die ervoor kiezen er voordeel uit te halen.

Het is in het algemeen niet mogelijk om gebruikerswachtwoorden over te switches naar het op MD5 gebaseerde algoritme dat wordt gebruikt om geheimen in te schakelen, omdat MD5 een eenrichtingshash is en het wachtwoord helemaal niet kan worden hersteld van de versleutelde gegevens. Om bepaalde verificatieprotocollen (met name CHAP) te kunnen ondersteunen, heeft het systeem toegang nodig tot de duidelijke tekst van gebruikerswachtwoorden, en moet het deze daarom opslaan met een omkeerbaar algoritme.

Bij belangrijke beheerproblemen zou het een niet-triviale taak zijn om over te switches naar een sterker omkeerbaar algoritme, zoals Data Encryption Standard (DES). Hoewel het eenvoudig zou zijn om Cisco IOS aan te passen om DES te gebruiken om wachtwoorden te versleutelen, zou er geen veiligheidsvoordeel in deze benadering zijn als alle Cisco IOS-systemen dezelfde DES-toets gebruikten. Als verschillende sleutels door verschillende systemen werden gebruikt, zou er een administratieve belasting worden geïntroduceerd voor alle Cisco IOS-netwerkbeheerders en zou de overdraagbaarheid van configuratiebestanden tussen systemen beschadigd raken. De vraag van de gebruiker naar een sterkere, omkeerbare wachtwoordversleuteling is gering geweest.

Gerelateerde informatie

- **Procedures voor wachtwoordherstel**
- **Cisco-handleiding over het versterken van Cisco IOS-apparaten**

- **Technische ondersteuning – Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.