Cisco IOS Password Encryption 정보 이해

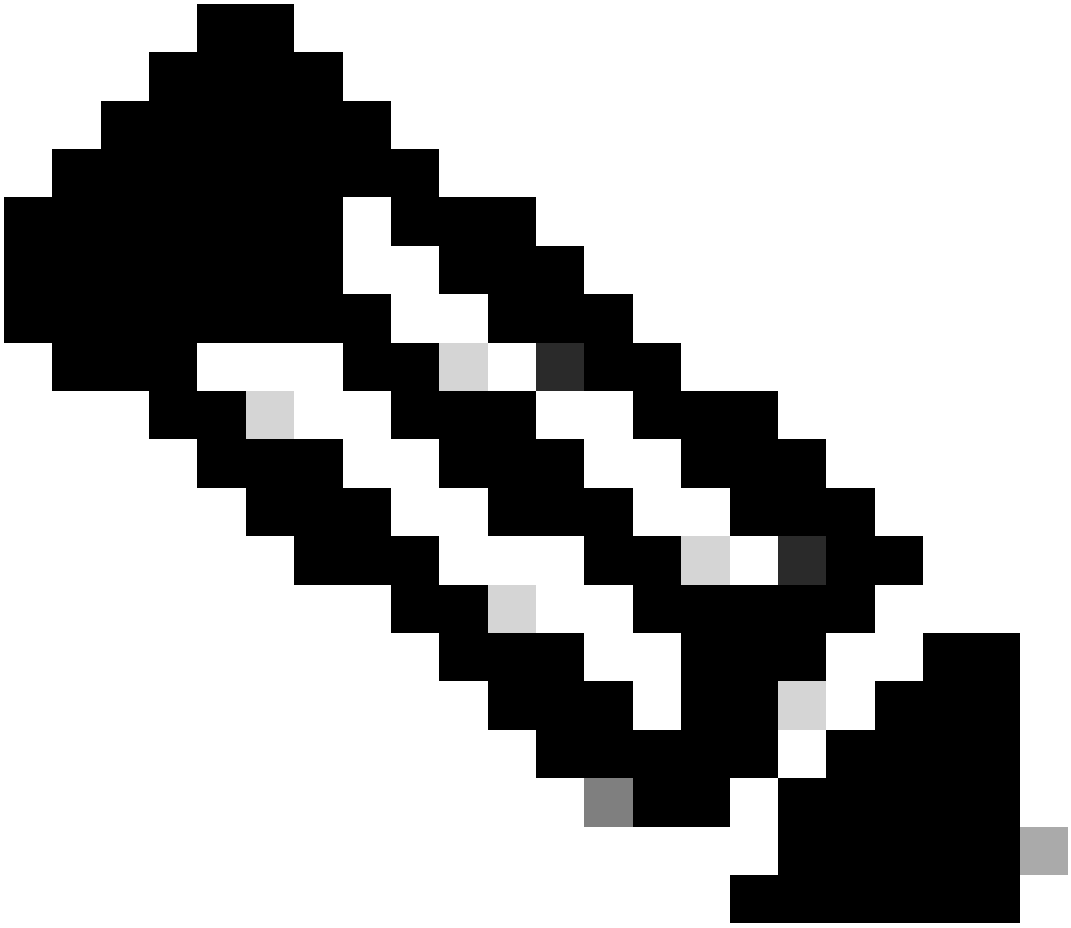
목차

소개

이 문서에서는 Cisco 비밀번호 암호화의 보안 모델과 해당 암호화의 보안 제한에 대해 설명합니다.

배경

Cisco 이외의 소스가 Cisco 설정 파일의 사용자 비밀번호(및 기타 비밀번호)의 암호를 해독하는 프로그램을 릴리스했습니다. 이 프로그램은 명령으로 설정된 비밀번호를 해독하지 **enable secret** 않습니다. Cisco 사용자 사이에 발생한 예기치 못한 문제로 인해 많은 사용자가 Cisco 비밀번호 암호화를 통해 제공하는 것보다 더 강력한 보안을 구현하려 한다는 의심을 받고 있습니다.



참고: 모든 Cisco IOS® 디바이스는 AAA(authentication, authorization, and accounting) 보안 모델을 구현하는 것이 좋습니다. AAA는 로컬, RADIUS 및 TACACS+ 데이터베이스를 사용할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사용자 암호

Cisco IOS 컨피그레이션 파일의 사용자 비밀번호 및 **enable secret**대부분의 다른 비밀번호는 최신 암호화 표준에서 매우 취약한 체계로 암호화됩니다.

Cisco는 암호 해독 프로그램을 배포하지 않지만 Cisco IOS 비밀번호에 대한 최소한 두 개의 다른 암호 해독 프로그램을 인터넷에서 사용할 수 있습니다. Cisco가 알고 있는 이러한 프로그램의 첫 번째 공개 릴리스는 1995년 초입니다. 아마추어 암호학자라면 아주 적은 노력으로 새로운 프로그램을 만들 수 있을 것으로 기대합니다.

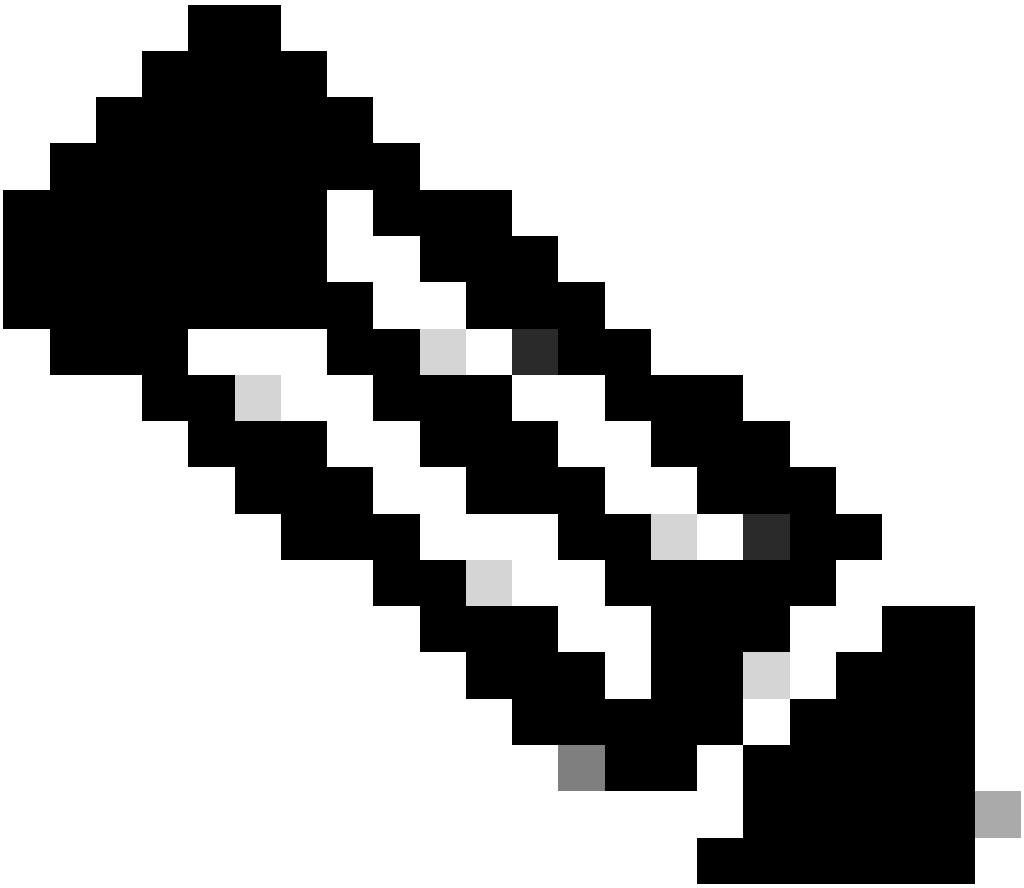
사용자 비밀번호를 위해 Cisco IOS에서 사용하는 체계는 결정적인 지능형 공격을 차단하기 위한 것이 아닙니다. 암호화 체계는 단순 스누핑 또는 스니핑에 의한 비밀번호 도용을 방지하기 위해 설계되었습니다. 이는 컨피그레이션 파일에서 비밀번호 크래킹 작업을 수행하는 사용자를 보호하기 위한 것이 아닙니다.

취약한 암호화 알고리즘 때문에, 사용자가 비밀번호를 포함하는 모든 컨피그레이션 파일을 비밀번호의 일반 텍스트 목록과 동일하게 민감한 정보로 취급하는 것은 항상 Cisco의 입장이었습니다.

enable secret 및 enable password 명령

이 enable password 명령은 더 이상 사용하지 않는 것이 좋습니다. 보안을 enable secret 강화하려면 명령을 사용합니다. 명령을 테스트할 수 **enable password** 있는 유일한 인스턴스는 디바이스가 명령을 지원하지 않는 부팅 모드에 있을 때뿐입니다enable secret.

Enable secrets(비밀 활성화)는 MD5 알고리즘으로 해시됩니다. 시스코의 모든 사람들이 아는 한, 설정 파일의 내용을 기반으로 enable secret을 복구하는 것은 불가능합니다(명확한 사전 공격 제외).



참고: 이는 로 설정된 비밀번호에만 적용되며enable secret 로 설정된 비밀번호에는 적용되지 **enable password**않습니다. 실제로 사용되는 암호화의 강점은 두 명령 간의 유일한 중요한 차이점입니다.

Enable secret을 지원하는 Cisco IOS 이미지는 무엇입니까?

정상 작동 모드의 **show version** 명령(전체 Cisco IOS 이미지)으로 부트 이미지를 확인하여 부트 이미지가 명령을 지원하는지 **enable secret** 확인합니다. 그럴 경우 를 **enable password**제거합니다. 부트 이미지가 지원되지 않는 경우 다음 주의 사항 **enable secret**을 참고하십시오.

- 물리적 보안이 유지되어 아무도 디바이스를 부트 이미지로 다시 로드할 수 없는 경우 enable 비밀번호를 사용하지 않아도 됩니다.

- 누군가가 디바이스에 물리적으로 액세스할 경우 부팅 이미지에 액세스할 필요 없이 디바이스 보안을 쉽게 파괴할 수 있습니다.

- 를 **enable password** 와 동일하게 설정할 경우 enable secret 를 와enable secret 같은 공격이 일어나기 쉽도록 **enable password**설정했습니다.

    - 부트 이미지**enable password** 가 지원되지 않기 때문에 다른 값으로 설정하면 라우터 관리자 **enable secret**는 명령을 지원하지 않는 ROM에서 자주 사용되지 않는 새 비밀번호를 기억해야 **enable secret** 합니다. 별도의 enable 비밀번호를 사용하여 관리자는 소프트웨어 업그레이드를 위해 다운타임을 강제로 수행할 때 비밀번호를 기억해야 하며, 이는 부팅 모드로 로그인해야 하는 유일한 이유입니다.

기타 비밀번호

Cisco IOS 컨피그레이션 파일의 거의 모든 비밀번호 및 기타 인증 문자열은 사용자 비밀번호에 사용되는 비약하고 가역적인 방식으로 암호화됩니다.

특정 비밀번호를 암호화하는 데 어떤 스키마가 사용되었는지 확인하려면 컨피그레이션 파일에서 암호화된 문자열 앞의 숫자를 확인합니다. 해당 숫자가 7이면 암호가 약한 알고리즘으로 암호화되었습니다. 숫자가 5이면 더 강력한 MD5 알고리즘으로 비밀번호가 해시되었습니다.

예를 들어, 설정 명령에서 다음을 수행합니다.

```
<#root>
```

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

enable secret은 MD5로 해시된 반면 명령에서는 다음과 같습니다.

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

암호가 약한 가역 알고리즘으로 암호화되었습니다.

설정 파일

전자 메일로 구성 정보를 보낼 때 유형 7 비밀번호의 구성을 삭제하십시오. 이 명령을 사용하면 show tech-support 기본적으로 정보가 지워집니다. 샘플 **show tech-support** 명령 출력이 여기에 표시됩니다.

<#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>
```

...

TFTP(Trivial File Transfer Protocol) 서버에 컨피그레이션 파일을 저장할 때 해당 파일이 사용 중이 아닐 때 해당 파일에 대한 권한을 변경하거나 방화벽에 배치합니다.

알고리즘을 변경할 수 있습니까?

시스코에서는 Cisco IOS 사용자 비밀번호에 대해 더욱 강력한 암호화 알고리즘을 지원할 계획이 없습니다. Cisco에서 향후 이러한 기능을 도입하기로 결정한 경우, 해당 기능은 이를 활용하기로 선택한 사용자에게 추가적인 관리 부담을 주게 됩니다.

MD5는 단방향 해시이고 암호화된 데이터에서 비밀번호를 복구할 수 없기 때문에 일반적으로 사용자 비밀번호를 enable 암호에 사용되는 MD5 기반 알고리즘으로 전환할 수 없습니다. 특정 인증 프로토콜(특히 CHAP)을 지원하려면 시스템은 사용자 비밀번호의 일반 텍스트에 액세스해야 하므로 이를 가역 알고리즘으로 저장해야 합니다.

키 관리 문제로 인해 DES(Data Encryption Standard)와 같은 보다 강력한 가역적 알고리즘으로 전환하는 것이 사소한 작업이 될 수 없습니다. DES를 사용하여 비밀번호를 암호화하도록 Cisco IOS를 수정하는 것은 쉽지만, 모든 Cisco IOS 시스템에서 동일한 DES 키를 사용한다면 이 접근 방식에서는 보안 이점이 없습니다. 시스템마다 다른 키가 사용된 경우, 모든 Cisco IOS 네트워크 관리자에게 관리 부담이 발생하며 시스템 간 설정 파일의 이동성이 손상됩니다. 강력한 가역적 비밀번호 암호화에 대한 사용자의 요구는 적었습니다.

관련 정보

- **암호 복구 절차**
- **Cisco IOS 디바이스를 강화하는 Cisco 가이드**

- **Technical Support - Cisco Systems**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.