ASA에서 SSH 서버 CBC 모드 암호 비활성화

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

문제

솔루션

소개

이 문서에서는 ASA에서 SSH 서버 CBC 모드 암호화를 비활성화하는 방법에 대해 설명합니다. 스캔 취약점 CVE-2008-5161에서는 CBC(Cipher Block Chaining) 모드에서 블록 암호 알고리즘을 사용하면 원격 공격자가 SSH 세션의 임의의 암호 텍스트 블록에서 알려지지 않은 벡터를 통해 특정 일반 텍스트 데이터를 더 쉽게 복구할 수 있다고 문서화되었습니다.

CBC(Cipher Block Chaining)는 암호 블록에 대한 작동 모드이며, 이 알고리즘은 블록 암호를 사용하여 기밀성이나 신뢰성과 같은 정보 서비스를 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA 플랫폼 아키텍처 적응형 보안 어플라이언스
- CBC(암호 블록 체인)

사용되는 구성 요소

이 문서의 정보는 Cisco ASA 5506(OS 9.6.1 포함)을 기반으로 합니다.

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.

문제

기본적으로 ASA CBC 모드에서는 ASA에서 활성화되며, 이는 고객 정보의 취약점이 될 수 있습니다.

솔루션

CSCum63371이 향상된 후 버전 9.1(7)에 ASA ssh 암호를 수정하는 기능이 도입되었지만 공식적으로 ssh 암호 암호화 및 ssh 암호 무결성 명령이 포함된 릴리스는 9.6.1입니다.

SSH에서 CBC 모드 암호를 비활성화하려면 다음 절차를 따르십시오.

ASA에서 "sh run all ssh"를 실행합니다.

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption medium
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

ssh cipher encryption medium 명령이 표시되면 이는 ASA가 기본적으로 ASA에 설정된 중간 및 고강도 암호를 사용함을 의미합니다.

ASA에서 사용 가능한 ssh 암호화 알고리즘을 보려면 show ssh ciphers 명령을 실행합니다.

```
ASA(config)# show ssh ciphers
Available SSH Encryption and Integrity Algorithms Encryption Algorithms:
        all:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        fips:    aes128-cbc   aes256-cbc
        high:    aes256-cbc   aes256-ctr
Integrity Algorithms:
        all:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
        low:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
        medium:  hmac-sha1    hmac-sha1-96
        fips:    hmac-sha1
        high:    hmac-sha1
```

출력은 사용 가능한 모든 암호화 알고리즘을 보여줍니다. 3des-cbc aes128-cbc aes192-cbc aes256-cbc128-ctr aes192-ctr aes256-ctr

ssh 컨피그레이션에서 사용할 수 있도록 CBC 모드를 비활성화하려면 다음 명령을 사용하여 사용할 암호화 알고리즘을 사용자 정의합니다.

```
ssh cipher encryption custom aes128-ctr:aes192-ctr:aes256-ctr
```

이 작업을 완료한 후 show run all ssh 명령을 실행합니다. 이제 ssh 암호화 컨피그레이션에서는 모든 알고리즘이 CTR 모드만 사용합니다.

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

마찬가지로, SSH 무결성 알고리즘은 ssh cipher integrity 명령을 사용하여 수정할 수 있습니다.

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.