일회용 비밀번호를 사용하여 RADIUS를 사용하는 ASA에서 SSH 인증 실패 트러블슈팅

목차

문제

CiscoSSH 스택이 사용하도록 설정된 경우 OTP(One-Time Password)를 사용하는 RADIUS(Remote Authentication Dial-In User Service)를 사용하는 ASA(Adaptive Security Appliance) 소프트웨어에 대한 SSH(Secure Shell) 액세스가 실패합니다.

다음 syslog 메시지가 생성됩니다.

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

환경

모든 조건이 일치하면 증상이 관찰됩니다.

- 단일 또는 다중 컨텍스트 모드의 ASA를 통한 보안 방화벽 1230 다른 하드웨어 플랫폼도 영향을 받습니다.
- RADIUS 서버는 SSH 인증에 사용됩니다.

<#root>

```
device#
```

show run | i aaa

```
aaa-server RAD-OTP protocol radius
aaa-server RAD-OTP (management) host 192.0.2.1
```

```
aaa-server RAD-OTP (management) host 192.0.2.2
aaa authentication ssh console RAD-OTP
```

- RADIUS 서버는 인증 성공을 위해 유효한 OTP 코드 또는 챌린지를 요청하고 요구합니다.
- CiscoSSH 스택은 ASA에서 활성화됩니다.
- 버전 9.19.1 이상에서는 CiscoSSH 스택이 기본적으로 활성화되며 no ssh stack cisco 명령을 사용하여 선택적으로 비활성화할 수 있습니다. 확인을 위해 show ssh 명령을 사용합니다.

<#root>

```
device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- 버전 9.23.1 이상에서는 이 스택을 비활성화하거나 확인할 수 없습니다.

해결

증상은 내부 랩에서 성공적으로 재현되고 Cisco 버그 ID CSCwt57790에서 추적됩니다.

영향을 받는 버전에서 다음 해결 옵션 중 하나를 사용합니다.

- SSH 연결에 로컬 인증을 사용합니다.
- RADIUS 서버에서 ASA에 대한 OTP 요구 사항을 비활성화합니다.
- 9.23 이전 버전에서는 no ssh stack cisco 명령을 사용하여 CiscoSSH 스택을 비활성화합니다. Cisco Secure Firewall ASA Series 명령 참조, S 명령을 검토하고 CiscoSSH 스택을 비활성화할 때의 잠재적인 영향을 평가합니다.

원인

인증 실패의 원인은 Cisco 버그 ID CSCwt57790입니다.

관련 콘텐츠

- Cisco 버그 ID CSCwi04513
- Cisco 버그 ID CSCwt57790
- Cisco Secure Firewall ASA Series 명령 참조, S 명령

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.