IPS 차단 설정을 통한 Cisco Secure Access Warn Action 재정의 동작

목차

문제

IPS가 활성화된 Cisco Secure Access의 액세스 정책(인터넷 액세스)에서 Warn 동작을 테스트할 때 Warn 동작이 IPS 차단 설정을 재정의하는 것처럼 보이는 예상치 못한 동작이 사용자에게 나타납니다. 특히, IPS 서명을 트리거할 URL에 액세스할 때(SERVER-WEBAPP /etc/passwd 파일 액세스 시도, GID-SID: 1-1122) 경고 페이지가 표시되고 사용자 확인 후 IPS가 트래픽을 차단하도록 구성되었음에도 불구하고 URL에 액세스할 수 있습니다.

이 구성에는 다음이 포함됩니다.

- 작업: 격리
- 침입 방지(IPS): Enable
- IPS/블록
- 서명: SERVER-WEBAPP /etc/passwd 파일 액세스 시도
- GID-SID: 1-1122

활동 검색 로그에 충돌하는 항목이 표시됩니다.

- IPS: (IPS: 차단)
- 웹: (웹: 허용 - 경고 페이지 표시됨)
- 웹: (웹: 허용 - 경고 액세스 후)

환경

- 제품: Cisco Secure Internet Access Advantage
- 기술: 보안 액세스
- 인터넷 액세스 및 경고 작업으로 구성된 액세스 정책
- 특정 시그니처에 대한 차단 작업으로 IPS 활성화

해결

이 동작은 액세스 정책의 경고 조치가 IPS 차단 설정보다 우선하는 Cisco Secure Access의 결함으로 확인되었습니다. 이 문제는 액세스 정책 경고 작업과 IPS 차단 기능 간의 상호 작용에 영향을 줍니다.

확인 단계

사용자 환경에서 이 동작을 확인하려면

1단계: 경고 작업으로 액세스 정책 구성 및 IPS 차단 활성화

- Action을 Isolate with Warn 동작으로 설정
- IPS(Intrusion Prevention) 활성화
- 차단 작업으로 IPS 구성
- 특정 시그니처 적용(예: SERVER-WEBAPP /etc/passwd 파일 액세스 시도, GID-SID: 1-1122)

2단계: IPS 서명을 트리거하는 URL에 액세스하여 컨피그레이션 테스트

```
https://example.com/etc/passwd
```

3단계: 행동 관찰

- 사용자에게 경고 페이지가 표시됩니다.
- 사용자는 경고를 확인한 후 진행할 수 있습니다.

- IPS 차단 컨피그레이션에도 불구하고 URL에 액세스할 수 있습니다.

4단계: 활동 검색 로그 확인

- IPS 블록 및 WEB 허용 항목이 모두 있는지 확인합니다.
- 충돌하는 로그 항목이 결함을 나타는지 확인합니다

현재 상태

이 동작은 현재 구현의 Warn(경고) 작업이 설계별로 IPS 차단 설정을 재정의하는 결함으로 확인되었습니다. GID-SID가 아닌 IPS 시그니처에서도 동일한 동작이 발생합니다. 1-1122. 이는 경고 작업이 구성된 경우 모든 IPS 시그니처에 영향을 주는 시스템 문제임을 나타냅니다.

이 결함에 대한 수정 계획과 시기는 아직 정해지지 않았다. 이 문제를 겪고 있는 조직은 보안 정책을 평가하고 엄격한 IPS 차단이 필요한 경우 대체 구성을 고려해야 합니다.

원인

근본 원인은 액세스 정책 경고 작업 처리가 IPS 블록 시행보다 우선하는 Cisco Secure Access의 결함입니다. 이 설계 결함에서는 사용자가 경고 확인 메커니즘을 통해 IPS 보안 제어를 우회할 수 있으므로 경고 작업을 구성할 때 IPS 차단 기능이 효과적으로 무효화됩니다.

Cisco Bug ID CSCwt39270은 이 사례와 관련이 있지만, 이 버그와 관찰된 Warn vs IPS 동작 간의 특정 관계에 대해서는 추가 조사가 필요합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.