Linux 커넥터 SELinux 정책 오류 해결

목차

소개

이 문서에서는 시스템의 SELinux 정책에서 커넥터가 시스템 활동을 모니터링하지 못하게 할 때 제기되는 결함에 대해 설명합니다.

배경 정보

SELinux가 활성화되어 있고 적용 모드에 있는 경우 커넥터에서는 이 규칙이 SELinux(Secure Enterprise Linux) 정책에 있어야 합니다.

```
allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };
```

이 규칙은 Red Hat 기반 시스템의 기본 SELinux 정책에 없습니다. 커넥터는 설치 또는 업그레이드 중에 `cisco-secure-bpf`라는 SELinux 정책 모듈을 설치하여 이 규칙을 추가하려고 합니다. 다음과 같은 경우 결함이 제기됩니다. `cisco` 보안 `bpf` 설치 및 로드에 실패하거나 비활성화됩니다. 이 결함이 커넥터에 의해 제기될 경우 사용자는 [Cisco Secure Endpoint Linux Connector Faults(Cisco Secure Endpoint Linux 커넥터 결함) 목록](#)에 설명된 대로 결함 19에 대한 알림을 받습니다.

적용 가능성

이 결함은 Connector를 새로 설치하거나 업그레이드한 후 또는 시스템의 SELinux 정책을 수정한 후에 제기될 수 있습니다.

운영 체제

- Red Hat Enterprise Linux 7
- CentOS 7
- Oracle Linux(RHCK/UEK) 7

커넥터 버전

- Linux 1.22.0 이상

해결

이 결함을 해결하기 위한 두 가지 방법이 있습니다.

1. 커넥터를 다시 설치하거나 업그레이드합니다.
2. SELinux 정책을 수동으로 수정합니다.

설치 종속성

두 방법 모두 SELinux 정책 모듈을 구축하고 로드하려면 시스템에 "policycoreutils-python" 패키지가 설치되어 있어야 합니다. 이 패키지를 설치하려면 이 명령을 실행하십시오.

```
yum install policycoreutils-python
```

커넥터 재설치 또는 업그레이드

cisco-secure-bpf라는 SELinux 정책 모듈 커넥터를 설치하거나 업그레이드하는 동안 필요한 SELinux 정책 수정을 제공하도록 설치됩니다. 이 해결 방법에 대해 커넥터를 표준 방식으로 재설치하거나 업그레이드하십시오.

수동으로 SELinux 정책 수정

시스템 관리자는 SELinux 정책 모듈을 수동으로 구축하고 로드하여 SELinux 정책을 수정해야 합니다. 필수 SELinux 정책 규칙을 로드하려면 다음 단계를 수행합니다.

1. cisco-secure-bpf.te라는 파일에 저장합니다.

```
module cisco-secure-bpf 1.0;
require {
type unconfined_service_t;
class bpf { map_create map_read map_write prog_load prog_run };
}
#============= unconfined_service_t ==============
allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };
```

2. 다음 명령을 사용하여 모듈을 빌드하고 로드합니다.

```
checkmodule -M -m -o "cisco-secure-bpf.mod" "cisco-secure-bpf.te"
semodule_package -o "cisco-secure-bpf.pp" -m "cisco-secure-bpf.mod"
semodule -i "cisco-secure-bpf.pp"
```

3. 결함을 제거하려면 Connector를 다시 시작합니다.

SELinux 정책 수정 확인

이 명령을 실행하여 `cisco-secure-bpf SELinux` 정책 모듈이 설치되었는지 확인합니다.

```
semodule -l | grep cisco-secure-bpf
```

출력이 "`cisco-secure-bpf 1.0`"을 보고하면 SELinux 정책 수정이 발생했습니다..

이 명령을 실행하여 필요한 SELinux 정책 규칙이 있는지 확인합니다.

```
sesearch -A | grep "unconfined_t unconfined_t : bpf"
```

출력이 "`allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };`"을 보고하면 커넥터를 다시 시작한 후 결함이 지워집니다.

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.