U-13

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- 불필요하거나 악의적인 파일에 SUID, SGID 설정 여부 점검

---

2. 점검 목적

- 불필요한 SUID, SGID 설정 제거로 악의적인 사용자의 권한상승을 방지하기 위한 목적

---

3. 보안 위협

- SUID, SGID 파일의 접근 권한이 적절하지 않을 경우 SUID, SGID 설정된 파 일로 특정 명령어를 실행하여 root 권한 획득 가능하다

---

4. 참고

- SUID : 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유자의 권한을 얻게 된다
- SGID : 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유 그룹의 권한을 얻게 된다
- 일반적으로 SUID 및 SGID 파일은 시스템 디렉토리에만 존재해야한다
  - 사용자 홈 디렉토리나 임시 디렉토리 등에서 발견된 파일은 불필요하거나 악의적일 가능성이 높습니다.

---

5. 취약 판단 기준

- 주요 실행 파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. 시스템 디렉토리 외의 위치에 있는 파일

```
find / \( -perm -4000 -o -perm -2000 \) -type f -not -path "/bin/*" -not -path "/sbin/*"
-not -path "/usr/bin/*" -not -path "/usr/sbin/*" -not -path "/lib/*" 2>/dev/null
```

6.2. 루트가 아닌 사용자가 소유한 파일

```
find / \( -perm -4000 -o -perm -2000 \) -type f ! -user root 2>/dev/null
```

6.3. 최근에 수정된 파일 (최근 7일 이내)

```
find / \( -perm -4000 -o -perm -2000 \) -type f -mtime -7 2>/dev/null
```

---

7. 조치 방법

7.1. 주요 파일에 불필요한 SUID/SGID가 설정된 경우 SUID/SGID를 제거 조치

```
chmod -s 파일이름
```