U-05

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- root 계정의 PATH 환경 변수에 “.”이(마침표, 현재 디렉터리) 포함되어 있는지 점검

---

2. 점검 목적

- 비인가자가 불법적으로 생성한 디렉터리 및 명령어를 우선으로 실행되지 않도록 설정하기 위한 목적

---

3. 보안 위협

- root 계정의 Path 환경 변수에 정상적인 관리자 명령어(예: ls, mv, cp등)의 디렉터리 경로보다 현재 디렉터리를 지칭하는 “.” 표시가 우선하면, 현재 디렉터리에 변조된 명령어를 삽입하여 관리자 명령어 입력 시 악의적인 기능이 실행 될 수 있다

---

4. 참고

- 환경 변수: 프로세스가 컴퓨터에서 동작하는 방식에 영향을 미치는 동적인 값들의 집합
- Path 환경 변수 : 실행 파일을 찾는 경로에 대한 변수

---

5. 취약 판단 기준

- PATH 환경 변수에 “.” 이 맨 앞이나 중간에 포함되어 있는 경우 취약하다고 판단

---

6. 점검 방법

6.1. Path 환경 변수 출력

```
echo $PATH
```

6.2. `.`이 PATH의 맨 앞 또는 중간에 포함되어 있는지 확인

```
echo $PATH | grep -E '(^\.|:\.:|^\.|:/\.(:|$))'
```

- 아무런 결과 값이 출력 되지 않으면 양호

---

7. 조치 방법

7.1. PATH 변수에서 `.` (현재 디렉토리)를 완전히 제거한다

```
export PATH=$(echo $PATH | sed -e 's/:\.//g' -e 's/^\.://')
```