U-09

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- /etc/hosts 파일의 권한 적절성 점검

---

2. 점검 목적

- /etc/hosts 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파 일 변조를 방지하기 위한 목적

---

3. 보안 위협

1. hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여, 이를 통해 정상적인 DNS를 우회하여 악성사이 트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있다
2. hosts파일에 소유자외 쓰기 권한이 부여된 경우, 일반사용자 권한으로 hosts 파일에 변조된 IP주소를 등록하여 정상적인 DNS를 방해하고 악성 사이트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있다

---

4. 참고

- /etc/hosts : IP 주소와 호스트 네임을 매핑하는 파일
  - 일반적으로 인터넷 통신 시 주소를 찾기 위해 도메인 네임 서비스(DNS)보다 hosts 파일을 먼저 참조한다
  - hosts 파일은 문자열 주소로부터 IP 주소를 수신받는 DNS 서버와는 달리, 파일 내에 직접 문자열 주소 와 IP 주소를 매칭하여 기록하며, DNS 서버 접근 이전에 확인하여 해당 문자열 주소가 목록에 존재할 시 그 문자열 주소에 해당하는 IP 주소로 연결한다
- 파밍(Pharming) : 사용자의 DNS 또는 hosts 파일을 번조함으로써 정상적인 사이트로 오인하여 접속하도록 유도한 뒤 개인정보를 훔치는 새로운 컴퓨터 범죄 수법

---

5. 취약 판단 기준

- /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 600 초과인 경우 취약하다고 판단

---

6. 점검 방법

6.1. /etc/hosts 파일 권한 확인

```
cd /etc
ls -al hosts
```

---

7. 조치 방법

7.1. 파일의 소유자 및 권한 변경 조치

```
chown root /etc/shadow
chmod 600 /etc/hosts
```

- 소유자 root
- 권한 600