



Photo by Krivec Ales from Pexels

## CodeEngn Basic RCE L01 Writeup



Daniel Smith

Feb 14 · 3 min read

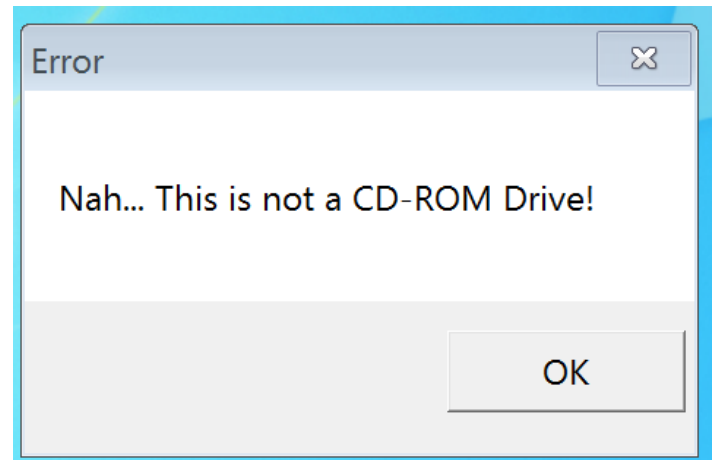
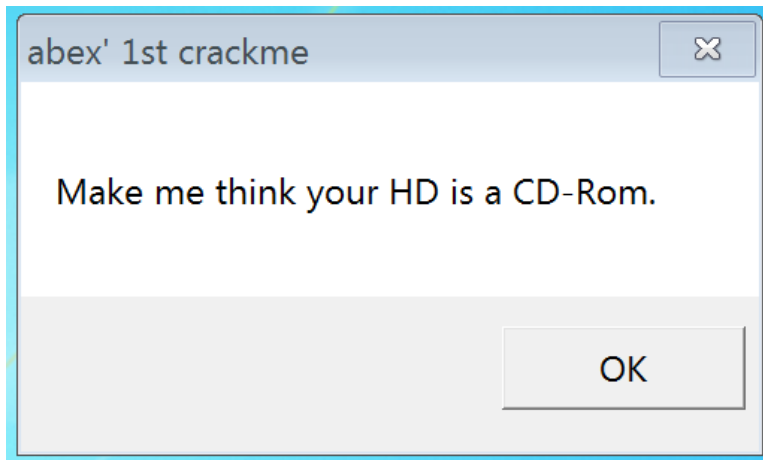
Let's start RCE

Filename: 01.exe

Description: HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리

턴값이 무엇이 되어야 하는가  
Author: abex

일단 프로그램을 실행시켜보자



flow ->

문제의 description 과 프로그램을 실행 시켜 보았을 때, 우리는 **GetDriveTypeA** 함수의 반환 값을 조작하여 프로그램이 HDD를 CD-Rom 으로 인지하도록 만드는 것이 목표라고 유추할 수 있다.

```

00401000 $ 6A 00 PUSH 0
00401002 . 68 00204000 PUSH 01.00402000
00401007 . 68 12204000 PUSH 01.00402012
0040100C . 6A 00 PUSH 0
0040100E . E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 . 68 94204000 PUSH 01.00402094
00401018 . E8 38000000 CALL <JMP.&KERNEL32.GetDriveTypeA>
0040101D . 46 INC ESI
0040101E . 48 DEC EAX
0040101F . EB 00 JMP SHORT 01.00401021
00401021 > 46 INC ESI
00401022 . 46 INC ESI
00401023 . 48 DEC EAX
00401024 . 3BC6 CMP EAX,ESI
00401026 . 74 15 JE SHORT 01.0040103D
00401028 . 6A 00 PUSH 0
0040102A . 68 35204000 PUSH 01.00402035
0040102F . 68 3B204000 PUSH 01.0040203B
00401034 . 6A 00 PUSH 0
00401036 . E8 26000000 CALL <JMP.&USER32.MessageBoxA>
0040103B . EB 13 JMP SHORT 01.00401050
0040103D > 6A 00 PUSH 0
0040103F . 68 5E204000 PUSH 01.0040205E
00401044 . 68 64204000 PUSH 01.00402064
00401049 . 6A 00 PUSH 0
0040104B . E8 11000000 CALL <JMP.&USER32.MessageBoxA>
00401050 > E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>

```

Style = MB\_OK|MB\_APPLMODAL  
Title = "abex' 1st crackme"  
Text = "Make me think your HD is a CD-Rom."  
hOwner = NULL  
MessageBoxA  
RootPathName = "c:\  
GetDriveTypeA

Style = MB\_OK|MB\_APPLMODAL  
Title = "Error"  
Text = "Nah... This is not a CD-ROM Drive!"  
hOwner = NULL  
MessageBoxA

Style = MB\_OK|MB\_APPLMODAL  
Title = "YEAH!"  
Text = "Ok, I really think that your HD is a CD-ROM! :p"  
hOwner = NULL  
MessageBoxA  
ExitProcess

전체 코드

살펴보니 실행 흐름은 GetDriveTypeA 함수의 반환 값에 의해서 실패 또는 성공 MessageBox 가 있는 곳으로 Jump 되는 것 같다.

CMP 명령 실행 직전 Register 상태를 확인하기 위해 해당 주소 (0x00401024) 에 BP 를 걸었다

```

PUSH 0
PUSH 01.00402000
PUSH 01.00402012
PUSH 0
CALL <JMP.&USER32.MessageBoxA>
PUSH 01.00402094
CALL <JMP.&KERNEL32.GetDriveTypeA>
INC ESI
DEC EAX

```

Registers (MMX)

EAX	00000003
ECX	76ED6360 ntdll.76ED6360
EDX	002F0174
EBX	7FFD3000
ESP	0012FF8C
EBP	0012FF94
ESI	00000000
EDI	00000000

GetDriveTypeA 함수 실행 후

GetDriveTypeA 을 호출한 뒤 나온 반환 값은 3(DRIVE\_FIXED)이다

00401000	\$ 6A 00	PUSH 0	Registers (MMX)
00401002	. 68 00204000	PUSH 01.00402000	EAX 00000001
00401007	. 68 12204000	PUSH 01.00402012	ECX 76ED6360 ntdll.76ED6360
0040100C	. 6A 00	PUSH 0	EDX 002F0174
0040100E	. E8 4E000000	CALL <JMP.&USER32.MessageBox>	EBX 7FFD3000
00401013	. 68 94204000	PUSH 01.00402094	ESP 0012FF8C
00401018	. E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	EBP 0012FF94
0040101D	46	INC ESI	ESI 00000003
0040101E	. 48	DEC EAX	EDI 00000000
0040101F	. EB 00	JMP SHORT 01.00401021	EIP 00401024 01.00401024
00401021	> 46	INC ESI	C 0 ES 0023 32bit 0(FFFFFFFF)
00401022	. 46	INC ESI	P 0 CS 001B 32bit 0(FFFFFFFF)
00401023	. 48	DEC EAX	A 0 SS 0023 32bit 0(FFFFFFFF)
00401024	. 3BC6	CMP EAX,ESI	Z 0 DS 0023 32bit 0(FFFFFFFF)
00401026	. 74 15	JE SHORT 01.0040103D	

EAX: 3 ESI: 3 -> EAX: 1 ESI: 3

그리고 CMP 명령이 실행되기 전에 반환 값이 3 에서 2가 깎여 1이 되었  
고, ESI 가 3이 되었다

CMP 명령에서 EAX, ESI 를 비교한 뒤, 각 Register 값이 서로 같다면 성공 MessageBox 로 Jump 하므로 반환 값을 5(DRIVE\_CDROM)로 바꾼다면 EAX 와 ESI 의 값이 서로 같아지므로 성공 MessageBox 가 출력될 것이다

GetDriveTypeA 에 대한 상세한 설명은 [MSDN](#)에 기술되어있는 문서를  
참고하면 된다

이제 문제를 해결해보자

0040101D	46	INC ESI
0040101E	48	DEC EAX
0040101F	EB 00	JMP SHORT 01.00401021
00401021	46	INC ESI
00401022	46	INC ESI
00401023	48	DEC EAX
00401024	. 3BC6	CMP EAX,ESI

패치 전

CMP 명령 이전의 명령들을 보다 보면 JMP 명령어가 2 byte를 차지하고 있는 것을 볼 수 있다

2 byte 의 크기라면 INC EAX 명령을 2번 삽입하여 기존의 EAX 의 값을 2 증가시킬 수 있다

```

0040101D 46      INC ESI
0040101E 48      DEC EAX
0040101F 40      INC EAX
00401020 40      INC EAX
00401021 46      INC ESI
00401022 46      INC ESI
00401023 48      DEC EAX
00401024 . 3BC6  CMP EAX,ESI

```

패치 후

Address	Disassembly	Comment
00401000	PUSH 0	
00401002	PUSH 01.00402000	
00401007	PUSH 01.00402012	
0040100C	PUSH 0	
0040100E	CALL <JMP.&USER32.Mess	
00401013	PUSH 01.00402094	
00401018	CALL <JMP.&KERNEL32.Ge	
0040101D	INC ESI	
0040101E	DEC EAX	
0040101F	INC EAX	
00401020	INC EAX	
00401021	INC ESI	
00401022	INC ESI	
00401023	DEC EAX	
00401024	CMP EAX,ESI	
00401026	JE SHORT 01.0040103D	
00401028	PUSH 0	
0040102A	PUSH 01.00402035	

Register	Value
EAX	00000003
ECX	76ED6360
EDX	00260174
EBX	7FFDD000
ESP	0012FF8C
EBP	0012FF94
ESI	00000003
EDI	00000000
EIP	00401024
C 0	ES 0023
P 1	CS 001B
A 0	SS 0023
Z 0	DS 0023
S 0	FS 003B
T 0	GS 0000

패치 후에 실행 시켰을때, EAX 와 ESI 의 값이 같아지므로 성공  
MessageBox 로 점프한다

. . .

잘못된 정보가 있을 경우, 이메일 또는 코멘트로 자유롭게 피드백을 남겨주시면 정말 감사드리겠습니다 (danielsmith0612@gmail.com)