**컴퓨터 보안**

[Fuzzing]

학번 : 12141579

학과 : 컴퓨터정보공학과

이름 : 윤찬미

연락처 : 010-9287-1679

E-mail : [cmmcme0604@gmail.com](mailto:cmmcme0604@gmail.com)

1. **Fuzzing 대상 프로그램**

**네이버 미디어 플레이어**

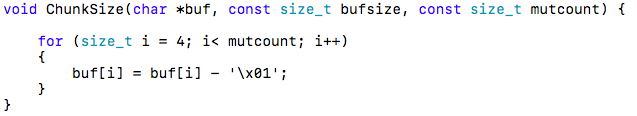
1. 네이버에서 개발되었기 때문에신뢰도가 높다.
2. 많은 사용자들이 사용하고 있다
3. 그로 인해 보안적 취약점을 찾았을 수 있을 것이라 예상된다

**2. 입력 파일 포맷 분석**

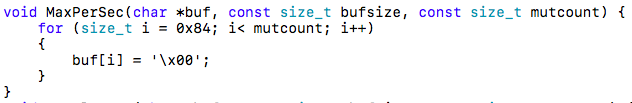
|  |  |  |  |
| --- | --- | --- | --- |
| 위치 | 이름 | 크기 | 의미 |
| 0x00 | chunkID | 4 | ”avih” |
| 0x04 | chunkSize | 4 | 헤더 8바이트를 제외한  데이터 크기. |
| 0x80 | MicroSecPerFrame | 4 | 프레임과 프레임 사이 시간 간격. 단위는 밀리초 |
| MaxBytesPerSec | 4 | 최대 초당 전송 바이트 수 |
| Reserved | 4 |  |
| Flags | 4 | 플래그, 인덱스 유무 등을 나타낸다 |
| TotalFrames | 4 | 총 프레임 수 |
| InitialFrames | 4 | 시작 프레임 |
| Streams | 4 | 스트림 개수. 하나의 오디오와 비디오가 있는 경우 스트림 수는 2 |
| SuggestedBufferSiz | 4 | 파일을 읽을 때 사용할 버퍼 크기 |
| Width | 4 | 이미지 폭. 픽셀 단위 |
| Height | 4 | 이미지 높이. 픽셀 단위 |
| Reserved | 16 |  |

1. **Fuzzing 계획**
2. 0x04 - ChunkSize 데이터의 크기를 변조시킨다.
3. 0x80 + 4 - MaxBytesPerSec 최대 초당 전송 바이트 수 → 최대 전송 바이트 수를 0으로 만들어 전송 할 수 없게 만든다.
4. 0x80 + 16 TotalFrames 총 프레임 수를 변조시킨다 → 해당 바이트를 아무런 값으로 나누어 주서 현재 프레임 수와 다르게 만든다.
5. **Fuzzing 접근 법 & 소스 코드**
6. mutate.avi를 만든다 buf에 org.avi의 내용을 그대로 옮겨 쓴다. 그 내용을 mutate.avi에도 써준다.
7. Fuzzing 함수로 buf의 값을 바꿔준다.
8. 바뀐 buf 값을 mutate.avi에 써준다.

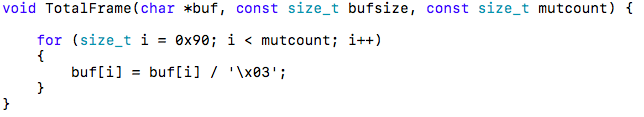
* fuzzing 접근은 입력파일 포맷 분석을 통해 알아낸 header의 값을 수정해준다.

1. 

chunksize는 헤더를 제외한 데이터의 크기이다. 헤더를 제외한 데이터의 크기를 작게 바꾸면 crash가 일어날 것이라고 생각되었다.

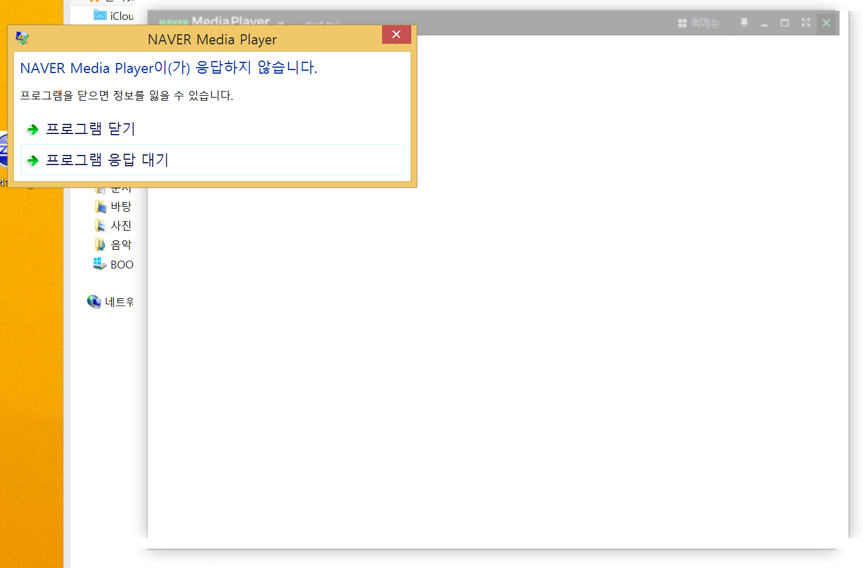
1. 

입력 파일 포맷을 보면 0x80 에서 두번째에 MaxBytePerSec 이 존재한다. 최대 전송 바이트 수를 0으로 만들면 최대로 전송 할 수 있는 값이 0이기 때문에 전송이 되지 않을 것이라고 예상하였다.

1. 

TotalFrame 값을 변조해준다.

1. **프로그램 실행 화면**

****

****

1. **Crash 발생여부**

* 결론적으론 Crash 가 발생되지 않았고 할 수 있다. 위의 캡쳐 화면처럼 crash가 발생한 경우도 가끔 있었지만, 다양한 AVI 파일을 시도해본 결과 발생되지 않은 파일이 더 많았다.
* 또한 여러가지 방법을 한꺼번에 시도했을 때만 Crash가 발생하였다.

1. **결론**

|  |  |
| --- | --- |
| Original AVI File | Mutate AVI File |
| 0x04 fuz%20(2)/원래1.PNG  fuz%20(2)/원래2.PNG  fuz%20(2)/원래3.PNG | 0x04 **fuz%20(2)/바뀜1.PNG**  fuz%20(2)/바꿈2.PNG  fuz%20(2)/바뀜3.PNG |

* 파일이 깨져서 정상적으로 재생이 되지 않았다. 동영상의 길이에 비례하여 매우 짧은 시간동안 동영상이 재생되지만 아무런 화면이 보이지 않았다. Mutate.avi의 값이 Org.avi 에서 달라진 것을 보아 소스코드는 틀리지 않았다는 것을 알 수 있다. Fuzzing 공격 방법을 여러가지를 섞어서 하면 가끔 crash가 발생하기도 하였지만 모든 경우에서 발생하진 않았다.

1. **시스템 사양**

1. Operating System : Window 8.1

2. IDE : Visual Studio 2015 community

3. Processor : 2.5 GHz intel Core i7

4. Memory : 16GB 1600 MHz DDR3

5. 언어 : C++11