Bug Hunting Challenge

임정원, 현성원

2014.04.03

PPT

- PPT는 **발표시작 15분 이후**부터 받을 수 있습니다.
- 발표 시간 이후엔 CODEGATE 공식 웹사이트!

http://cloud.sweetchip.kr/codegate/

목차

- 소개
- 프로젝트
  - 프로젝트 소개
  - 프로젝트 목표
  - 프로젝트 진행방법
  - 작성한 구조
  - 발견한 Crash 구조
  - 분석
- 결론

프로젝트 팀원 소개

- 심준보 (passket)
- BOB 2기 멘토
- BlackPerl Security 연구원

- 임정원 (setuid0)
- 선린 인터넷 고등학교
- CodeRed 소속

- 최재승
- 서울대학교 정보보안 연구 동아리 Guardian 소속
- CTF팀 Alternatives 소속

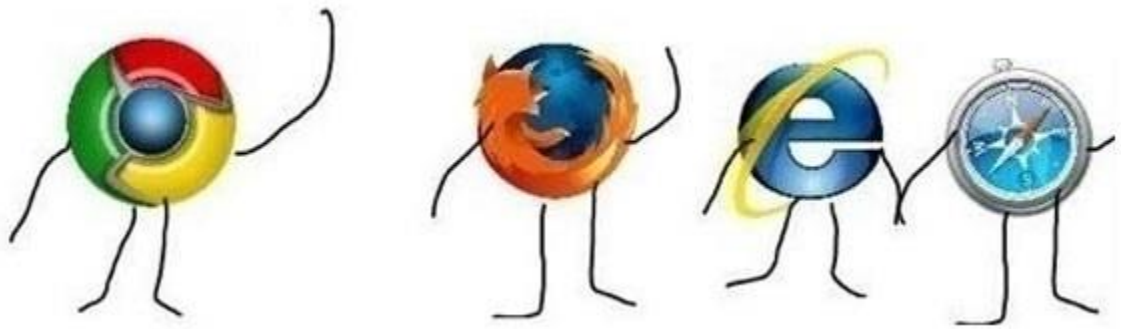
- 현성원 (sweetchip)
- 세종대학교 정보보호학과
- HackerSchool - Wiseguys

프로젝트 소개

- 프로젝트 명 : 국내외 소프트웨어의 0-day 취약점 발견 및 연구
- 기간 : BOB 2기 경연단계 (1월 ~ 2월 28일)
- 목표 : IE, Chrome, Java, Flash 등 세계적으로 많이 사용되는 프로그램의 취약점 발견
- 목적 : 비교적 국내 프로그램보다 매우 높은 보안 수준을 가진 프로그램의 취약점을 발견할 수 있는 능력과 경험

프로젝트 진행 방법

- 프로젝트 진행 방법
  - 처음 프로젝트 계획 당시 브라우저의 경우 UAF 취약점을 발견을 목표로 함.
  - UAF 버그가 발생하는 원리를 공부하기 위하여 프로젝트 이전에 발표되었던 Internet Explorer의 UAF 취약점 Proof Of Concept Code를 다시 분석하고 보고서를 작성.
  - 브라우저를 공격할 수 있는 방법을 배우기 위하여 오류를 유발할 만한 코드를 손으로 직접 작성.



DOM

- 단순히 DOM Tree 구조를 복잡하게 한 뒤, 구조를 바꾸는 과정에서 발생하는 버그가 여전히 보고되는 것을 확인.
- 잘 알려지지 않고 DOM Tree 구조에 영향을 줄 수 있는 함수 탐색.
- DOM 트리 구조가 삭제될 때 하위 Element들을 모두 삭제하는 함수에서 중복 삭제 오류가 있을 것으로 추측.
- Element들의 상속 구조를 순환하도록 제작 하여 use-after-free 또는 double-free 류의 버그가 발생할 수 있을 것으로 추측.

Event Handler

- HTML 파일에서 복잡한 구조의 Element들을 생성
- 생성한 복잡한 구조에 있는 값을 참조할 만한 이벤트 핸들러를 다수 등록
  - 이벤트 핸들러에는 구조를 바꾸거나 삭제하는 등 구조에 직접적인 영향을 주도록 한다.
  - 참조할 만한 이벤트 핸들러 외에도 트리 구조가 바뀔 때 발생하는 이벤트, etc
- 등록된 이벤트 핸들러가 작동 될 수 있도록 이벤트를 트리거 시킨다.
- Example : DOMNodeInserted, etc . . .

Web Worker

- 웹 브라우저의 JavaScript 엔진은 Race-Condition 취약점이 발생하지 않도록 싱글 쓰레드로 동작하지만 최신 기술인 web worker로 쓰레드를 추가로 생성하여 작업을 시킬 수 있다.
- DOM은 멀티 쓰레드에 적합하게 설계되지 않았기 때문에 여러 쓰레드를 생성하고 DOM Tree에 변화를 주는 등 다양한 방법을 이용하여 접근하면 취약점을 발견할 수 있을 것이라고 기대하고 접근하였다.

Html5

- 최근 Pwn2Own 대회에서 공격된 Mozilla FireFox에서 IndexedDB의 IDBkey 취약점이 발견되었음.
- 최근에 개발되어 비교적 예전부터 있던 기능보다 안정성 검증이 부족할 것으로 추정되는 html5에서 새롭게 추가된 기능들을 이용하면 취약점을 찾을 수 있을 것으로 기대.
- Example : IndexedDB, Canvas, LocalStorage, etc . . .

Iframe

- Iframe의 하위접근이 가능하다는 점을 확인.
- A, B라는 html이 있다면 A.html에 다수의 컨텐츠를 삽입.
- 일정 주기마다 html 요소 전체에 대해 select() 함수를 호출.
- B.html에서 A.html을 로딩하는 Iframe 태그 삽입.
- B.html에서 A.html에 있는 document 전체를 unselect() method를 호출.

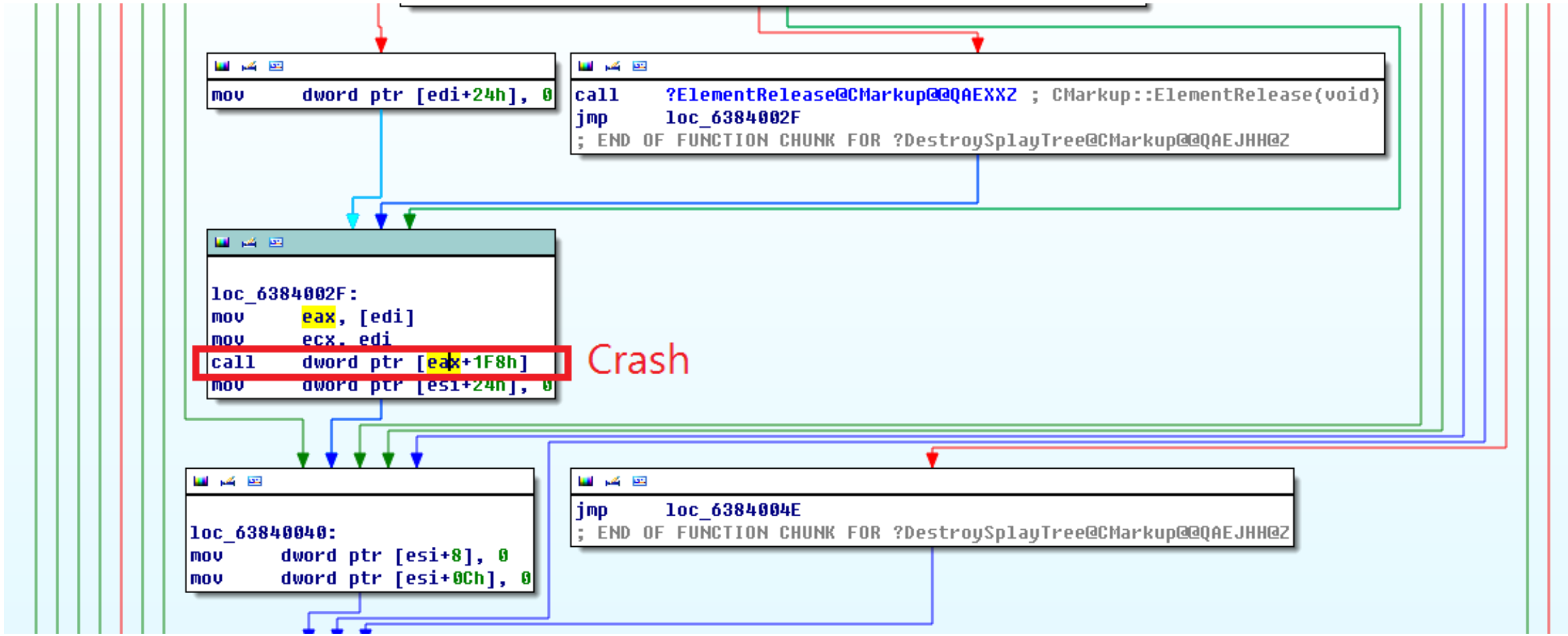
Stack Overflow

- 프로젝트 중 발견된 Crash

```
(fa4.1d9c): Stack overflow - code c00000fd (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for MSHTML.dll -
MSHTML+0xd8223:
53988223 56              push    esi
0:008:x86> r
eax=78e61813 ebx=087f1af0 ecx=087f1af0 edx=087f1b48 esi=043833ac edi=087f1b34
eip=53988223 esp=04382f38 ebp=043831a4 iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210202
MSHTML+0xd8223:
53988223 56              push    esi
```

- Document Body에 Element 상속 반복
- Exploitable 하지 않은 Crash로 잠정 결론

Use-After-Free



Use-After-Free

- 취약점 발견 아이디어
  - 프로젝트 기간 중 나온 iframe 아이디어를 적용하여 UAF 로 추정되는 Crash를 발견
- 취약점이 발생하는 원인
  - 부모 문서에서 iframe의 DOM tree를 접근할 수 있다는 점을 이용.
  - DOM 트리가 삭제될 때 DOM 트리에는 다양한 객체들이 올 수 있음
  - 부모 문서에서 iframe에 접근하면서 iframe 내부에서는 selectAll 함수를 이용하여 삭제 과정을 혼란을 주면 삭제할 객체 목록에 잘못된 객체가 들어감

Use-After-Free

- 취약점 트리거 방법
  - 다른 페이지로 이동할 때 브라우저는 DOM의 모든 객체를 삭제한다.
  - 그 과정에서 모든 Element를 참조하게 되는데 그 순간 Free된 객체의 vtable을 참조하게 되어서 크래시가 발생한다.

분석

- Windbg Script를 이용하여 Memory의 Allocate와 Free 상황을 모니터링
- jscript9.dll의 math 함수에 브레이크 포인트를 설정.
- javascript 코드에서 math 함수를 사용하여 어느 부분에서 Crash가 발생하는지 알 수 있음.
- Example
  - bu jscript9!Js::Math::Atan2 ".printf ₩"%mu₩", poi(poi(esp+14)+c);.echo;g" // windbg script
  - bu101 ntdll!RtlFreeHeap "j (poi(esp+c)!=0) '.printf ₩"free(0x%p) from (%p)₩", poi(esp+c), poi(esp); .echo; g'; 'g';
  - ##
  - Math.atan2(0xbadc0de,"LOG : going to call setInterval()"); // javascript code
  - Math.atan2(0xbadc0de,"LOG : finshed loading another page");

```
alloc(0x28) = 0x07c37c30 from 7078f6a0
alloc(0x60) = 0x07da52d0 from 707c55f6
alloc(0x8) = 0x07c9b358 from 708b3140
free(0x07c37c30) from (706340c6)
free(0x07c379f0) from (706340c6)
free(0x07c36df0) from (706340c6)
LOG : going to load another page
LOG : finshed loading another page
```

Ms14-010


심준보
2월 13일
http://www.microsoft.com/ko-kr/security/pc-security/bulletins/201402.aspx
확인해보세요
2014년 2월 Microsoft 보안 업데이트
2014년 2월의 최신 컴퓨터 보안 업데이트를 확인하고 다운로드하십시오. 스파이웨어 방지 및 스팸 방지 프로그램을 사용한 컴퓨터 보호에 관한 도움말을 읽으십시오.
WWW.MICROSOFT.COM
좋아요 · 댓글 달기 · 공유하기
모두 읽음
현성원 헐
2월 13일 오전 10:56 · 좋아요
임정원 패치됐네요.. ㅜㅜ
2월 13일 오전 11:32 · 좋아요
심준보 ㅋㅋㅋㅋㅋ 아놔 슈발
2월 13일 오전 11:32 · 좋아요
현성원 저 사람들중에 한명이..
2월 13일 오전 11:33 · 좋아요
최재승 ;;;
2월 13일 오후 1:55 · 좋아요

Ms14-010

Microsoft Security Bulletin MS14-010 - 긴급

Internet Explorer 누적 보안 업데이트 (2909921)

게시된 날짜: 2014년 2월 12일 수요일

버전: 1.0

일반 정보

요약

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건과 비공개로 보고된 취약점 23건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

프로젝트 결론

- 프로젝트 기간 중 진행 한 과정
  - windbg를 이용하여 PageHeap을 설정하고 Free된 메모리의 크기를 조사한다.
  - Free된 크기만큼 다시 문자열 또는 페이로드를 할당.
  - 조작된 vtable를 참조하게 되어서 흐름 변경 가능.
- 완전한 Exploit을 위해선
  - 적용된 SandBox 를 깰 수 있는 취약점 1개와 ASLR을 우회할 수 있는 Information Leak 이 가능한 취약점 1건이 추가로 필요.

프로젝트 결론

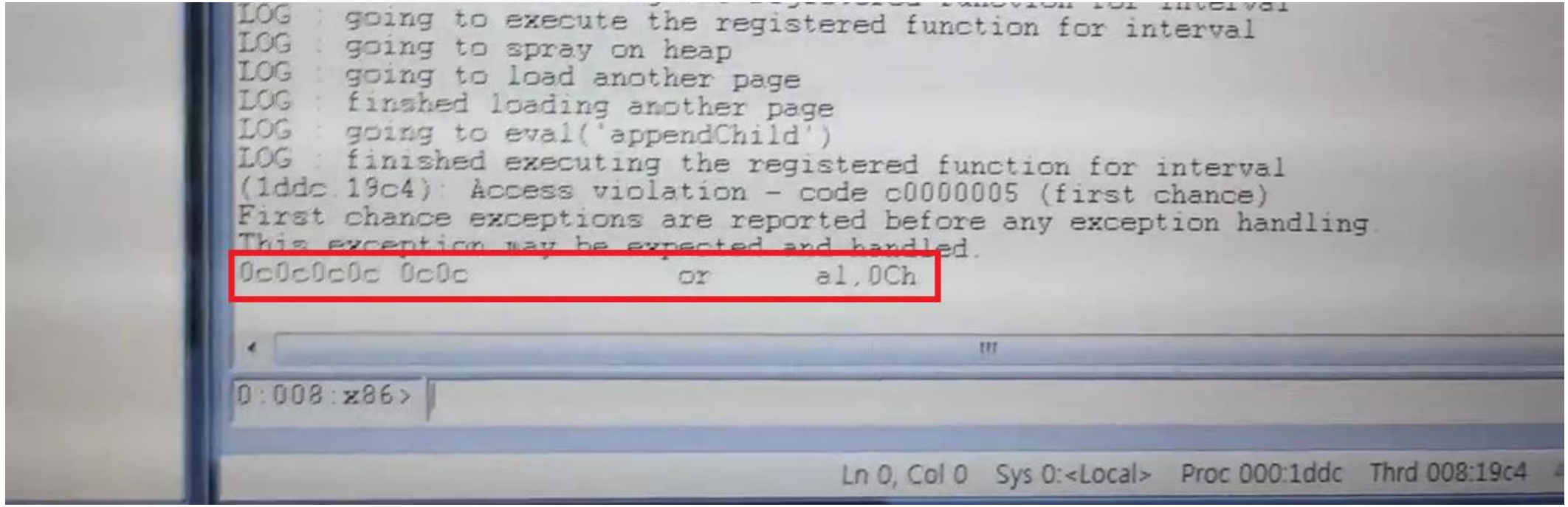
- 프로젝트 기간 중 진행 한 과정

```
(b64.11a4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00610061 ebx=07d62250 ecx=04bada28 edx=07c17ce0 esi=00f96570 edi=04bada28
eip=707e0033 esp=032fbed8 ebp=032fbf50 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
MSHTML!CMarkup::DestroySplayTree+0x8c1:
707e0033 ff90f8010000      call      dword ptr [eax+1F8h] ds:002b:00610259=????????
```

  - [사진] 조작된 Vtable 을 참조한 사진

프로젝트 결론

- DEMO (EIP CONTROL)



프로젝트 결론

- 프로젝트 결과
  - IE, Chrome, Firefox, Safari 에 대한 Stack Overflow, Access violation 유발 Bug 발견
  - IE11에 대한 Use-After-Free Bug 발견
  - 버그를 이용하여 EIP Control을 하는 Proof of concept Code 작성 성공.
  - 프로젝트 기간 중 발견한 Internet Explorer 11 취약점 분석 보고서 작성 완료

프로젝트 결론

- 프로젝트 결과
  - 현재 EIP 컨트롤 POC코드로는 Remote Code Execution이 불가능 하다.
  - ASLR에 의하여 exploit 성공률이 현저하게 떨어진다.
  - Sandbox 우회를 위한 Sandbox Escape 취약점 1개가 추가 적으로 필요하다.
  - 위를 보완할 경우 실제 사이버 공격에 이용 할 수 있는 무기 형태로 만들 수 있다.

프로젝트 결론

- 결론
  - 프로젝트를 진행하면서 실제로 브라우저의 취약점을 발견 해볼 수 있었음.
  - 브라우저에서 오작동을 발생 시킬 수 있을 만한 코드를 작성 할 능력을 기를 수 있는 기회가 되었음.

감사합니다.