

ISSN 1738-9593
제20권 1호

www.ksii.or.kr



2019 춘계학술 발표대회

논문집

4월 26일(금) ~ 27일(토)

동국대학교 서울캠퍼스 사회과학관



주최: 사단법인 한국인터넷정보학회

주관: 동국대학교 서울캠퍼스

후원: SK스토아(주), (주)카카오, (주)LGCNS, (주)아이티센

www.ksii.or.kr



KOREAN SOCIETY FOR INTERNET INFORMATION
사단법인 한국인터넷정보학회

B. 인터넷보안 (좌장 : 조규상 교수(동양대))

B-1 IoT 환경에 적합한 경량 블록암호 성능 분석	53
김의진, 곽진(아주대)	
B-2 의료정보접근을 위한 IoT 상황정보기반으로한 자동인증시스템의 서비스 모델 구현	55
함규성, 주수중(원광대)	
B-3 ☆ ICS 사이버 공격 동향 분석	57
고영민, 김득훈, 곽진(아주대)	
B-4 Frida를 이용한 안드로이드 악성앱 분석기술 연구	59
이석훈, 류재철(충남대)	
B-5 ☆ 악성코드 작성자 그룹 식별을 위한 저자 클러스터링을 적용한 특징 추출	61
신건윤, 한명묵(가천대)	
B-6 최신 핀테크 서비스 현황 및 보안 동향 분석	63
고주성, 곽진(아주대)	
B-7 웹 브라우저 취약점 사례 분석 및 대응 방안	65
이민경, 최슬기, 곽진(아주대)	

C. 인터넷미디어 (좌장 : 이우찬 교수(인천대))

C-1 Conditional GAN을 이용한 단일 영상에서의 그림자 제거 방법	71
윤희진, 전준철(경기대)	
C-2 빅데이터 분석과 AHP를 이용한 악성 댓글 분류	73
김진우, 조혜인, 이봉규(연세대)	
C-3 U-Net을 이용한 간 분할 방법	75
김강직, 전준철(경기대)	
C-4 인터넷 먹방 프로그램의 긍정적 및 부정적 효과	77
지양슈에진, 황하성(동국대)	

B. 인터넷보안

웹 브라우저 취약점 사례 분석 및 대응 방안

이민경*, 최슬기**, 박진***

*.***아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과 정보보호응용및보증연구실

e-mail : *leemkl@ajou.ac.kr, **skchoi.isaa@gmail.com, ***security@ajou.ac.kr

Case Analysis and Countermeasure of Web Browser Vulnerabilities

Min Kyung Lee*, Seul-Ki Choi**, Jin Kwak***

***Department of Cyber Security, Ajou University

**ISAA Lab., Department of Computer Engineering, Ajou University

요 약

웹 브라우저는 인터넷을 통해 정보를 검색하고 이용하는 데 필수적으로 활용되는 도구로써 많이 이용하고 있다. 이러한 웹 브라우저의 기능들은 지속적으로 개선 및 확장되고 있으며, 최신의 웹 브라우저들은 HTML 정보를 출력하는 단순한 기능뿐만 아니라 동영상 재생 및 문서 뷰어 등의 기능을 제공할 수 있는 확장된 형태의 프로그램 및 서비스까지 제공함으로써 사용자에게 다양한 편리성을 제공하고 있다. 하지만, 사용자의 편리성이 향상된 만큼 웹 브라우저의 취약점 또한 증가하게 되었으며, 취약점을 악용한 다양한 보안위협들이 발생하게 되었다. 이에 따라, 웹 브라우저의 보안성 향상을 위한 다양한 연구들이 진행되고 있다. 본 논문에서는 웹 브라우저에서 발생한 최신 취약점 사례에 대한 분석과 안전한 웹 브라우저 사용을 위한 대응방안을 제안한다.

1. 서 론

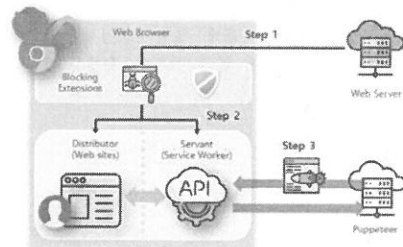
웹 브라우저는 인터넷망에서 정보를 검색하고 이용하는 데 필수적으로 활용되는 도구로써 많이 이용되고 있다. 이를 통해 사용자들은 동영상 재생, 메일 송·수신 및 자료 업·다운로드 등 다양한 활동이 가능하다. Fossbytes에서 보도된 내용에 따르면, 최근에는 여러 웹 브라우저가 개발되고 있고 지속적인 업데이트를 통해 확장프로그램, 시크릿 모드와 북마크 관리등과 같은 여러 기능이 추가되고 있다. 하지만 편리성이 증가한 만큼 확장프로그램 및 API를 통한 웹 브라우저의 취약점 또한 증가하고 있으며, 이를 악용한 보안위협들이 발생하게 되었다[1].

따라서, 본 논문에서는 최신 웹 브라우저들에서 발생한 취약점 사례들을 분석하고 이와 같은 취약점 및 보안 위협에 대응하기 위해서 최신 웹 브라우저들이 제공하고 있는 공통적인 보안 설정에 대한 분석 및 대응방안을 제시한다.

2. 웹 브라우저 취약점 사례 분석

2.1 마리오네트

마리오네트라는 공격은 최신 웹 브라우저들이 지원하는 기존 HTML5 API를 사용하고 그중에서도 Service Workers라는 기능을 사용한다. Service Workers는 특정 계산을 별도의 스레드로 이동시킴으로써[2], 웹 페이지 창과 분리되어 실행할 수 있다. 따라서, 오프라인 기간 동안 사용자에게 서비스를 제공하는 브라우저 내 캐싱 프로세서로 사용된다. 마리오네트의 구성요소는 세 가지로, Distributor, Servant 그리고 Puppeteer가 존재한다[3].



(그림 1) 마리오네트 개요

Step 1. Webpage fetch

사용자가 Distributor인 어떤 웹사이트를 방문하게 되면 Distributor는 웹 페이지의 리소스와 함께 Servant에게 JavaScript 코드를 전달한다.

Step 2. Webpage rendering

웹 페이지가 rendering 되는 도중에, Servant는 User의 브라우저에 배치된다. Servant가 컨트롤 서버인 Puppeteer와 원격 커맨드와 함께 통신 채널을 구축한다.

Step 3. Communication channel

Servant는 초기 작업 세트를 요청한다. 공격자는 Puppeteer를 이용해 Servant에게 원격 명령을 전송하고 Servant는 Puppeteer로부터 악성 스크립트를 받아 수행한다.

위와 같이 마리오네트 공격을 이용해서 공격자들은 원격으로 실행시킬 수 있는 악성코드를 사용자의 PC에 설치함으로써 DDoS 공격, 패스워드 크래킹 그리고 악성 데이터 호스팅 등이 다양한 악성행위를 수행하는데 활용할 수 있다[3].

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

2.2 Chrome UaF 취약점

2019년도 3월 1일에 Chrome 72.0.3626.121버전에서 발생한 취약점 CVE-2019-5786을 방지하기 위한 패치를 실시하였다[4]. 해당 취약점은 파일리더 API에서 발견된 취약점으로 UaF(Use after Free) 취약점이다[4]. UaF는 동적 할당된 힙 메모리를 free하고 다시 재사용 할 때 발생하는 취약점으로, 특수하게 조작된 웹 페이지로 사용자를 우회시킬 때 실행되는 공격방법이다[5].

따라서 Chrome UaF 취약점을 통해 공격자는 브라우저에서 임의 코드 실행을 가능하게 만들어줌으로써 프로그램들을 설치하거나 데이터에 대한 열람, 변경 또는 삭제 명령을 수행할 수 있으며, 심지어는 계정을 새로 생성하는 등 다양한 공격을 수행할 수 있는 취약점이다[4].

2.3 Internet Explorer 취약점

CVE-2019-0609는 2019년도 3월에 패치된 취약점으로써, 이용자가 특수하게 제작된 악성 웹 페이지를 열람할 경우, 원격코드실행을 허용하고 보안기능을 우회할 수 있는 취약점이다[5]. 이 취약점은 브라우저의 메모리에 있는 개체를 처리하는 방식에 존재하는 것으로 만약 공격이 발생한다면 메모리가 손상되어 공격자가 임의로 코드를 실행할 수 있다. 그리고 공격자는 API에서 ActiveX Control을 포함 시킬 수도 있다. 이를 통해 공격자는 현재 사용자와 동일한 권한을 얻을 수 있고 데이터에 대한 열람, 변경, 삭제가 가능하며, 전체 사용자 권한으로 새 계정을 생성할 수 있는 등 다양한 공격 기능을 수행할 수 있다[6].

3. 대응방안

본 장에서는 다양한 웹 브라우저들에 대한 보안성 향상을 위한 공통적인 보안 설정들[7]에 대한 분석과 새로운 보안 기능을 제시한다.

□ 기본 브라우저 설정

인증된 브라우저를 기본 브라우저로 변경한다. 사용자가 인증하지 않았거나 안전성이 검증되지 않은 웹 브라우저가 사용자의 PC에 설치되어도 이러한 웹 브라우저를 통한 인터넷 연결을 방지하기 위하여 다양한 애플리케이션에서 사용자가 설정한 기본 브라우저를 사용할 수 있도록 한다.

□ 업데이트 자동 설치

브라우저 업데이트를 자동적으로 진행하도록 설정한다. 브라우저 취약점으로 인한 업데이트가 지속적으로 발생하고 있기 때문에 자동 업데이트로 설정하는 것을 권고한다.

□ 원하지 않는 팝업 차단

원하지 않는 팝업창을 차단한다. 공격자가 위조해놓은 악성 웹페이지를 새 창 또는 새 탭으로 여는 경우를 사전에 방지할 수 있다.

□ 원하지 않는 애드온 차단

원하지 않는 확장프로그램을 설치하는 것을 차단한다. 악성 행위에 활용될 수 있는 확장프로그램을 자동으로 설치하는 것을 방지함으로써 악성코드 감염 시도를 줄일 수 있다.

□ 패스워드 저장 설정 해제

패스워드를 브라우저에 저장하지 않는다. 패스워드를 저장할 경우 편리성은 증가한다. 하지만 만약 브라우저가 악성코드에 감염되어 웹 브라우저에 저장된 패스워드를 공격자가 쉽게 사용할 수 있기 때문에 이러한 위험을 방지하기 위하여 패스워드는 브라우저에 저장해두지 않는다.

□ 쿠키 파일의 안전한 관리

쿠키는 사용자가 웹사이트를 방문할 때, 자동으로 생성되는 작은 임시 파일이다. 이러한 쿠키파일은 웹 사이트를 이용하기 위하여 여러 가지 목적으로 활용될 수 있는데 사용자의 세션 정보와 같이 사용자 인증 등의 중요한 역할로 사용될 수 있다. 따라서 이러한 쿠키파일에 대하여 접근제어나 암호화 같이 안전하게 관리할 수 있는 수단을 활용하여야 한다.

□ 확장프로그램 및 Service Worker에 대한 평판 조회

HTML5 API인 Service Worker를 사용하는 마리오네트와 같이 웹 브라우저에 추가적으로 설치 및 이용되는 유형의 공격에 대응하기 위해서 확장프로그램 및 API에 대한 다양한 사용자들의 평판 정보를 수집하여 관리하는 방안을 제안한다.

확장프로그램 및 Service Worker를 사용하고 있는 사용자들로부터 주기적으로 해당 프로그램 및 서비스에 대한 신뢰도를 평가하거나 혹은 해당 확장프로그램 및 Service Worker를 삭제 또는 설치 거부를 수행했을 때, 삭제 및 설치 거부 등의 사유 정보를 수집함으로써 확장프로그램 및 Service Worker에 대한 관리를 수행함으로써 안전성과 신뢰성을 확보한다.

4. 결 론

웹 브라우저는 사용자의 편의성을 위해 지속적으로 다양한 기능 등을 추가하며 발전해나가고 있다. 하지만 확장프로그램 및 Service Worker 등 웹 브라우징 외에 추가적인 기능을 수행하는 애플리케이션들이 개발됨으로써 이들의 취약점을 이용한 보안 위협들이 등장하게 되었다. 따라서 본 논문에서는 웹 브라우저에서 발생할 수 있는 마리오네트 공격뿐만 아니라 Chrome 및 IE 발생한 보안 취약점들에 대하여 분석하였으며, 안전한 웹 브라우저 환경을 위한 보안 설정들에 대한 분석과 확장프로그램 및 Service Worker에 대한 평판 조회와 같은 새로운 보안 기능을 제안하였다.

향후에는 웹 브라우저에서 발생하는 취약점들에 대한 통계조사를 통해 더욱 발전된 형태의 보안 기능들을 연구하고자 한다.

참 고 문 헌

- [1] OWASP, "Top 10 Vulnerabilities in web applications", 2017.
- [2] Google, "4.2.3 서비스 작업자 소개", support.google.com
- [3] Panagiotis Papadopoulos, "Master of Web Puppets: Abusing Web Browsers for Persistent and Stealthy Computation", Feb 2019.
- [4] CIS(Center for Internet Security), "A Vulnerability in Google Chrome Could Allow for Arbitrary Code Execution", March 2019
- [5] 한국인터넷진흥원(KISA), "MS 3월 보안 위협에 따른 정기 보안 업데이트 권고", March 2019.
- [6] Microsoft, "Scripting Engine Memory Corruption Vulnerability(CVE-2019-0609)", March 2019.
- [7] UCSC(UC Santa Cruz), "Web Browser Secure Settings", Sep 2018.