

무선공유기 웹 인터페이스에서의 XSS 취약점¹

김지혜, 윤희주, 박다란, 이해영
서울여자대학교 정보보호학과
e-mail : haelee@swu.ac.kr

XSS Vulnerabilities in Web Interfaces of Wireless Routers

Ji Hye Kim, Heejoo Yoon, Da Ran Park, Hae Young Lee
Dept. of Information Security, Seoul Women's University

요약

사물인터넷 시대가 도래함에 따라, 사물과 인터넷 간의 연결을 위한 무선 공유기의 활용이 증가하고 있다. 그러나 무선 공유기의 보안 취약점을 악용한 침해 사고도 지속적으로 발생하고 있어, 공유기 보안이 심각한 문제로 대두된 상황이다. 본 논문에서는 국내에서 사용되는 3 사의 공유기가 제공하는 웹 기반 관리자 인터페이스에서 발견된 크로스 사이트 스크립팅(cross-site scripting) 취약점을 분석한다. 발견된 취약점을 기반으로, 가능한 공격 시나리오와 패치 발표 이전까지 임시 대응할 수 있는 방법을 제시한다.

1. 서론

최근 무선 공유기(wireless routers, 이하 공유기)의 보안 취약점(security vulnerabilities)을 악용(exploitation)한 침해 사고가 지속적으로 보고되고 있다. 2014년 11월에는, 1,633 대의 공유기에 악성 코드가 감염되고, 감염된 공유기가 SK 브로드밴드 서초·동작 DNS(domain name system)에 대해 분산 서비스 거부(distributed denial-of-service) 공격을 수행함으로써 서비스 장애가 발생하기도 하였으며[1], 공유기 DNS를 변조하여 파밍(pharming) 사이트로 접속을 유도하는 사례도 지속적으로 보고되고 있다[2]. 이에 정부는 미래창조과학부, 통신사, 공유기 제조업체 및 한국인터넷진흥원 간의 협력을 통해 공유기 보안 강화 대책을 마련하여 추진 중이며[1], 후속 대책으로 공유기 취약점 신고 포상 제도를 운영하기도 하였다[3].

대부분의 공유기는 편리한 설정 및 관리를 위한 웹 어플리케이션(web application) 기반의 인터페이스를 제공한다. 그러므로 공유기의 웹 인터페이스에도 웹 어플리케이션 취약점이 존재할 가능성이 있다. 특히 크로스 사이트 스크립팅(cross-site scripting, 이하 XSS)은 가장 광범위하게 분포되어 있는 웹 어플리케이션 취약점이므로[4], 공유기의 인터페이스 내에 존재할 가능성이 매우 높다. XSS는 웹 어플리케이션이 입력 받은 값을 검증하지 않고 브라우저로 보내는 경우 발생할 수 있으며, 이를 악용하여 공격자의 악성 스크립트가 실행되게 함으로써, 세션 탈취, 사이트 변조, 포워딩 등의 공격을 수행할 수 있다[5].

본 논문에서는 국내에서 사용되고 있는 3 사 공유

기의 웹 인터페이스에서 XSS 취약점을 분석하고, 가능한 공격 시나리오를 제시한다. 또한, 발견된 취약점으로 인한 피해를 줄일 수 있도록, 패치 이전까지의 임시 대응을 위한 권고 사항도 제시한다. 현재 모든 제품에 대한 패치가 발표된 것은 아니므로, 제조사 및 상세 취약점을 논문에 수록하지는 않았으며, 발표에서 공개할 예정이다.

2. 크로스 사이트 스크립팅(XSS)

XSS 취약점은 취약한 웹 사이트에 악성 스크립트를 포함할 수 있는 손쉬운 방법 중 하나로, 공격자들이 가장 많이 선호하는 방식 중 하나이다[5]. XSS 공격은 크게 3 가지 형태로 수행될 수 있다. 첫째, 저장(stored) XSS에서는, 대상 사이트의 취약한 페이지에 악성 스크립트를 (데이터베이스 등을 통해) 영구적으로 저장해 놓는다. 사용자가 해당 페이지를 방문하면, 저장된 스크립트가 실행되면서 공격이 수행된다. 둘째, 반사(reflected) XSS은 웹 어플리케이션이 입력 받은 값을 검사하지 않고, 다시 브라우저로 전송하는(즉, 반사) 취약점을 활용한다. 즉, 사용자가 악성 스크립트를 포함한 URL(Uniform Resource Locator)을 요청하도록 유도하고, 이를 요청하면 웹 어플리케이션이 해당 스크립트를 반사함으로써 공격이 수행된다. 셋째, DOM(document object model)[6] 기반 XSS에서는 클라이언트 측에서 입력 값을 검사하지 않고, DOM을 통해 HTML 문서에 그대로 반영하는 취약점을 활용한다. 반사 XSS와 유사하게, 사용자가 악성 스크립트를 포함한 URL을 요청하도록 유도하고, 이를 요청하면 HTML 문서에 스크립트가 반

¹ 이 논문은 2015년도 정부(교육부)의 재원으로 한국과학창의재단(대학단계프로그램 (URP)지원사업)의 지원을 받아 수행된 연구임.

영되어 실행됨으로써 공격이 수행된다.

3. 주요 공유기에서의 XSS 취약점

A사의 공유기에서는 공유기에 연결된 공격자가 관리자 권한이 없어도 악성 스크립트를 공유기 로그에 삽입할 수 있고(즉, 저장 XSS), 공유기 관리자가 그 페이지를 열면 스크립트가 실행되는 취약점²이 발견되었다. 해당 취약점은 대상 공유기가 제공하는 크로스 사이트 요청 위조(cross-site request forgery, 이하 CSRF)를 탐지 기능의 문제로부터 기인한다. 대상 공유기는 CSRF로 의심되는 HTTP(Hypertext Transfer Protocol) 요청을 탐지하면, 해당 요청이 어디에서 왔는지를 보여주기 위하여, HTTP 요청 헤더 [7] 중 ‘Referer’ 필드의 내용(즉, 이전 페이지 URL)을 별도의 검증 없이 로그에 저장한다. 또한, 관리자가 로그 페이지를 열 때에도, 저장된 내용을 여과 없이 출력한다. 그러므로 (그림 1)과 같이 Referer 필드에 악성 스크립트를 삽입하여 HTTP 요청을 보냄으로써 해당 스크립트를 로그에 저장할 수 있으며, 관리자가 로그 페이지를 여는 순간 스크립트가 실행된다.

```
telnet x.x.x.x 80
GET /x?x=x HTTP/1.1
Referer:
<script>parent.frames[2].location="http://www.kisa.or.kr/";</script>
```

(그림 1) 공격용 HTTP 요청 예제



(그림 2) 취약점을 이용한 메뉴 조작 예제

해당 취약점을 악용하여 (그림 2)와 같이 프레임으로 구성된 메뉴를 조작할 수 있으며, 이를 통해 가짜 펌웨어(firmware)를 설치하도록 유도할 수 있다. 또한, 페이지를 패밍 페이지로 포워딩함으로써, 다시 로그인(login) 정보를 입력하도록 유도하는 것도 가능하다.

² 한국인터넷진흥원을 통해 신고 및 검증이 완료된 취약점(15-342)임.

능하다. 그러므로 로그 페이지를 열어본 이후에는, 모든 문서나 하이퍼링크의 URL 을 유심히 관찰할 필요가 있다. 패치 이전의 임시 대응으로, 공유기의 로깅 기능을 끄거나, CSRF 탐지 기능을 끄는 방법도 있다. 다만, 이 경우에는 또 다른 취약점에 노출될 가능성도 존재한다.

B사의 공유기에서는 DOM 기반 XSS 취약점이 발견되었다. 해당 취약점은 (그림 3)과 같이 클라이언트 측 자바스크립트에서 현재 문서의 URL 을 참조하고, URL의 값들을 별도의 검증 없이 DOM 을 기반으로 HTML 문서에 반영하는 문제로부터 기인한다. 그러므로 (그림 4)와 같이 URL의 특정 부분에 악성 스크립트를 넣어 입력하면, 클라이언트 측 자바스크립트 엔진에 의해 해당 스크립트가 문서에 삽입 및 실행되게 된다. 연구진의 검증 과정에서, 스크립트는 마이크로소프트 인터넷 익스플로러에서만 실행되었으며, 모질라 파이어폭스나 구글 크롬에서는 실행되지 않았다.

```
// ...
var url = document.location.toString();
var cmd = url.split("?");
// ...
var kind = cmd[1].split("%3b");
// ...
document.getElementById("x").innerHTML
+= "(" + kind[2] + ")";
// ...
```

(그림 3) 소스 코드 일부

```
http://x.x.x.x/x?x%3bx%3b<iframe
src="http://warning.or.kr/"></iframe>%3bx
```

(그림 4) 공격용 URL 예제



(그림 4) 취약점을 이용한 iframe 삽입 예제

해당 취약점을 악용하여 (그림 5)와 같이 아이프레임(iframe)을 삽입할 수 있으며, 패밍 페이지로 포워딩하여 계정 탈취 또는 가짜 펌웨어 다운로드로 이어지도록 유도하는 것도 가능하다. 물론 스크립트가 저장된 것이 아니므로, URL에 주의를 기울임으로써 피해를 예방할 수 있다. 그러나 특정 설정 값 등으로 이를 저장할 수 있다면, 더욱 정교한 공격으로 이어질 수도 있을 것이다. 패치 이전까지는 공유기 URL이나 내부 IP URL에 대해서 항상 확인을 해 볼 필요

가 있다.

C 사의 공유기에서는 반사 XSS 취약점이 발견되었다. 해당 취약점은 대상 공유기 내에서 실제 사용되지 않는 것으로 보이는 XML 관련 웹 어플리케이션의 문제점으로부터 기인한다. (그림 6)의 위의 같은 악성 스크립트가 POST 내용으로 담긴 URL 요청을 공유기에게 보내면, 웹 어플리케이션이 아래와 같이 해당 스크립트가 담긴 XML 페이지를 반환하였다. 연구진의 검증 과정에서, 해당 취약점이 일반적인 브라우저에서는 동작하지 않았으며, 웹 어플리케이션 취약점 스캐너인 IBM Security AppScan[8]과 크롬의 부가 기능인 Advanced REST Client[9]에서만 확인이 가능하였다. 그러나 취약점을 가진 웹 어플리케이션이 존재하는 만큼, 패치 이전까지는 공유기 URL이나 내부 IP URL에 대해서 주의를 기울일 필요가 있다. 향후 스크립트의 저장이 가능한 부분을 찾을 수 있다면, 심각한 공격으로 이어질 수도 있을 것이다.

```
x=x<abc%20xmlns:xyz='http://www.w3.org/1999/xhtml'><xyz:body%20onload='alert(716)' /></abc>&x=x&x=x
<?xml version="1.0" encoding="utf-8"?>
<...>x<abc
xmlns:xyz='http://www.w3.org/1999/xhtml'
><xyz:body
onload='alert(716)' /></abc><...>
```

(그림 6) 공격용 POST 내용(위) 및 응답(아래) 예제

4. 결론 및 향후 연구

본 논문에서는 국내에서 사용되고 있는 주요 공유기에서의 XSS 취약점을 분석하였으며, 이를 기반으로 공격 시나리오와 임시 대응 방법을 제시하였다. 사물인터넷(Internet of Things) 시대로 진입함에 따라, 공유기의 활용은 더욱 늘어날 것이며, 공유기 보안이 심각한 문제로 대두될 것이다[3]. 현재 공유기는 별도의 보안 인증 없이 제작 및 유통되고 있으며, 보안 패치, 백신 프로그램 등 별도의 보안 대책을 적용하기 어려운 상태이다 [1]. 그러므로 공유기 관리자는 공유기 보안을 항상 고려해야만 하며, 펌웨어를 항상 최신으로 유지될 수 있도록 노력할 필요가 있다.

향후 연구로는 공유기에서 XSS 외의 웹 어플리케이션 취약점(예를 들어, CSRF)에 대해서 조사할 예정이다. 또한, 본 연구에서는 5 종의 공유기에 대하여 취약점 점검을 수행하였는데, 다른 종류의 공유기에 대해서도 취약점 점검을 수행할 예정이다. 마지막으로 발견된 취약점을 기반으로 임시 대응 기법에 대한 연구를 수행할 계획이다.

참고문헌

- [1] “미래부, 공유기 보안 강화대책 발표,” 미래창조과학부 보도자료, 2015.03.
- [2] 김무열, 류소준, 최근 피싱, 패밍 기법을 이용한 금융정보탈취 동향, 한국인터넷진흥원, 2014.
- [3] “공유기 해킹 꼼짝마! 취약점 집중 신고 기간

운영,” 한국인터넷진흥원 보도자료, 2015.04.

- [4] “OWASP Top 10 - 2013,” OWASP, 2013.
- [5] 성윤기, “크로스 사이트 스크립팅(XSS) 공격 종류 및 대응 방법,” *Internet & Security Focus*, 2013.11.
- [6] *Document Object Model (DOM) Technical Reports*, W3C.
- [7] R. Fielding, J. Reschke, “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing,” IETF, Jun. 2014.
- [8] IBM Security AppScan. www.ibm.com/software/products/en/appscan
- [9] Advanced REST Client. <http://developer.myob.com/resources/tools/>