

Lighttpd 웹 서버 취약점 사례 분석

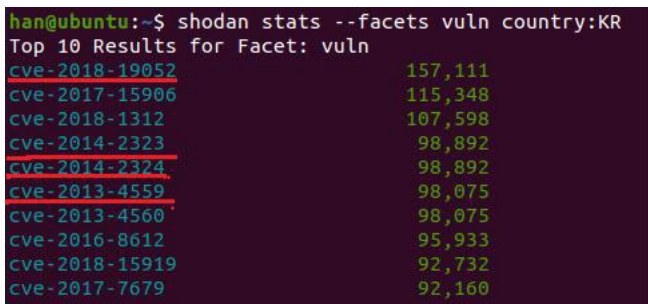
Lighttpd Web Server Vulnerability Case Analysis

요 약

lighttpd는 아파치와 같은 다른 웹 서버보다 훨씬 적은 메모리를 사용하면서도 CPU 부하를 관리하며 일반적으로 다른 웹 서버보다 속도가 빠른 서버이다. 2021년 4월 기준, 한국에서 가장 많이 노출되고 있는 취약점 TOP 10 중 무려 5개(1위, 4위, 5위, 6위, 7위)가 lighttpd 관련 취약점이었다. 그렇기 때문에 본 논문에서는 lighttpd에 대해 빈번하게 발생하는 취약점은 어떠한 이유로 발생하는지 사례를 통해 직접 구현 및 분석을 하고 그에 대한 해결 방안을 제시할 것이다.

1. 서 론

lighttpd는 웹 2.0에서 동작하는 웹 서버 어플리케이션으로써 적은 자원을 사용하여 높은 성능을 내는 웹서버로서 고안되었다. [1]
이 웹 서버는 고성능 환경에 최적화된 안전하고, 빠르고, 호환성이 뛰어나며 매우 유연한 웹 서버이다. lighttpd의 어원은 'light'+ 'httpd'의 합성어으로써, 어원 그대로 이것은 아파치와 같은 다른 웹서버보다 훨씬 적은 메모리를 사용하면서도 CPU 부하를 관리하며 일반적으로 다른 웹 서버보다 속도가 빠르다. YouTube, Wikipedia, Sourceforge와 같은 많은 웹사이트들에서 이 lighttpd를 사용하고 있다. [2]
2007년 4월 NetCraft 집계 웹 서버 순위 5위에 등록된 바 있으며 Alexa의 최상위 250개 사이트 중 5개 사이트가 랭크되었다.
2021년 4월 기준, 쇼단(shodan)을 이용해 한국에서 가장 많이 노출되고 있는 취약점을 검색해 봤을 때, TOP 10 중 무려 5개(1위, 4위, 5위, 6위, 7위)가 lighttpd 관련 취약점이었다.



Top 10 Results for Facet: vuln	
cve-2018-19052	157,111
cve-2017-15906	115,348
cve-2018-1312	107,598
cve-2014-2323	98,892
cve-2014-2324	98,892
cve-2013-4559	98,075
cve-2013-4560	98,075
cve-2016-8612	95,933
cve-2018-15919	92,732
cve-2017-7679	92,160

그림 1 쇼단(Shodan)을 이용한 국내 취약점 사례 수 검색 결과

그렇기 때문에 lighttpd에 관련된 취약점 사례를 선택해 분석하고 대처방안을 제시하려 한다. 취약점 사례는 상위

취약점 2개인 CVE-2018-19052(국내 취약점 1위 - 157,111건), CVE-2014-2323(국내 취약점 4위 - 98,892건)를 분석하려고 한다.

2. 환경 구축

2.1 Linux ubuntu 설치

CVE-2018-19052는 2018년 11월에 보고되었고, CVE-2014-2323은 2014년 3월에 보고 되었다. 그렇기 때문에 그 전에 나온 버전인 13.10 버전을 설치해 테스트하려 했으나, 최신 버전인 20.04 LTS 버전에서도 실행 해본 결과 취약점 테스트를 할 수 있기에 20.04 LTS 버전을 이용하였다.

2.2 lighttpd 설치

CVE-2018-19052는 1.4.50 이전 버전에서 발생하는 이슈이고 CVE-2014-2323은 1.4.35 이전 버전에서 발생하는 취약점이다. 따라서 두 조건을 모두 만족하는 1.4.34 버전을 설치하였다.

2.3 DB(mysql) 설치

CVE-2014-2323에 해당하는 SQL injection 버그를 테스트하기 위해 database의 한 종류인 mysql을 설치하여 lighttpd 서버와 연동하였다.

2.4 lighttpd 웹 서버를 기반으로 웹사이트 구축

lighttpd는 .htaccess 파일을 지원하지 않으므로 모든 설정을 lighttpd.conf 파일 혹은 그것이 포함하는 파일에 명시할 필요가 있다. 따라서 lighttpd.conf를 설정하고 간단한 html 파일과 image 파일 등을 넣어 테스트할 웹사이트를 구축하였다.[3]

3. 사례별 공격 실습

3.1 CVE-2018-19052[4]

이 취약점은 CWE-22[5]로써 path traversal(경로 이동)에 해당 하는 lighttpd.conf로 설정을 할 때 서버 모듈에서 mod_alias를 사용하고, mod_dirlisting 기능을 활성화하고, alias url을 적용했을 때 취약점이 발생하는 환경이 만들어진다.

이때 url alias 를 사용한 주소 끝에 ‘..’를 붙이면 그 상위 폴더로 이동할 수 있게 된다.

```
server.modules = (
    "mod_alias",
)
```

그림 2 mod_alias 모듈 적용

```
server.dir-listing = "enable"
dir-listing.activate= "enable"
```

그림 3 dir-listing 설정

다음 ‘/var/www/html’폴더를 메인으로 하는 웹사이트를 lighttpd 서버를 사용하여 구축하였다. 이때 ‘/test’를 url로 받으면 var/www/html/gogo/my_folder/test_for_this/’폴더로 이동하게 alising 하였다. 이때 ‘ip주소:port번호/test’로 입력을 받으면

var/www/html/gogo/my_folder/test_for_this/index.html’이 열린다. 하지만 ‘ip주소:port번호/test..’가 입력이 되면 ‘var/www/html/gogo/my_folder/test_for_this/..’가 적용이 되어 ‘var/www/html/gogo/my_folder/’로 이동하게 된다. 그러면 경로를 볼 수 있는 페이지가 열려 의도치 않은 다른 페이지로 이동할 수 있게 된다.

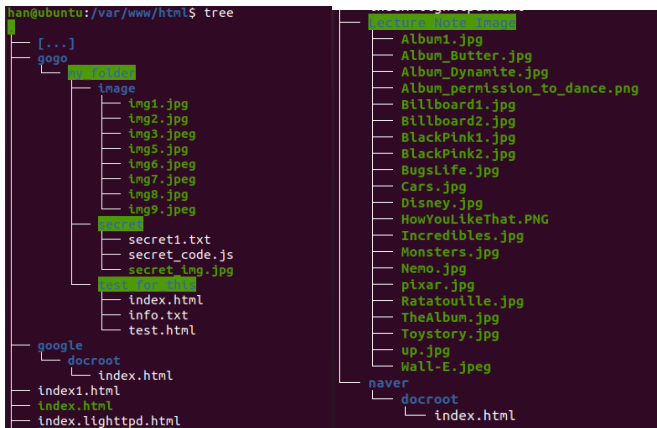


그림 4,5 메인폴더 기준 하위 파일 계층

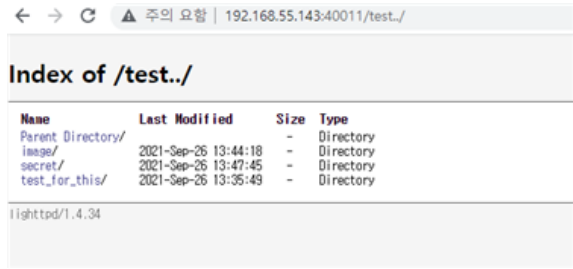


그림 5 취약점 노출 결과

3.2 CVE-2014-2323[6]

이 취약점은 CWE-89[7]로써 SQL injection에 해당하는 취약점이다. SQL query를 쓰기 때문에 mysql을 따로 설치해 앞에서 구축한 웹 환경에 DB를 연결해주었다. 그 후 lighttpd.conf에서 환경설정 할 때 서버 모듈에 ‘mod_mysql_vhost’를 추가해주고, mysql-vhost.db, mysql-vhost.user, mysql-vhost.pass, mysql-vhost.hostname, mysql-vhost.port 등 mysql 데이터베이스에 대한 설정을 해준다.[8]

```
server.modules = (
    "mod_mysql_vhost",
)
```

그림 6 mod_mysql_vhost 모듈 적용

```
mysql-vhost.db = "lighttpd"
mysql-vhost.user = "user01"
mysql-vhost.pass = "user01"
#mysql-vhost.sock = "/tmp/mysql.sock"
mysql-vhost.sql = "SELECT docroot FROM domains WHERE '?';"
mysql-vhost.hostname = "localhost"
mysql-vhost.port = 3306
```

그림 7 mysql-vhost 관련 환경 설정 적용

이 때 mysql-vhost.sql에 SQL query문을 설정하는데 이것이 취약점의 원인이 된다. 이것을 원격 공격자가 request_check_hostname과 관련된

host name을 이용해 임의의 SQL commands를 실행할 수 있다.

‘/var/www/html’폴더를 메인으로 하는 웹사이트를 lighttpd 서버를 사용하여 구축하여 mysql_vhost 환경 설정을 다 마친다. 이 때 curl 명령어를 사용해 curl --header “Host: []”; DROP TABLE domains;--”와 같이 HTTP Request를 보낸다. 이렇게 되면 mysql-vhost.sql에 의해 “SELECT docroot FROM domains WHERE ‘; DROP TABLE domains;--’;”와 같이 실행되어 domains 테이블이 삭제된다.

```
mysql> show tables;
+-----+
| Tables_in_lighttpd |
+-----+
| domains             |
+-----+
1 row in set (0.00 sec)

mysql> show tables;
Empty set (0.00 sec)
```

그림 8,9 SQL injection 수행 전후 DB 상태

4. 사례별 시큐어 코딩

4.1 CVE-2018-19052

Src/mod_alias.c 파일 안에 alias가 적용될 문자 끝에 '..'나 './'가 포함되나 확인된 후 이것이 존재할 경우 403 Forbidden으로 HTTP 상태를 리턴하게 해준다.

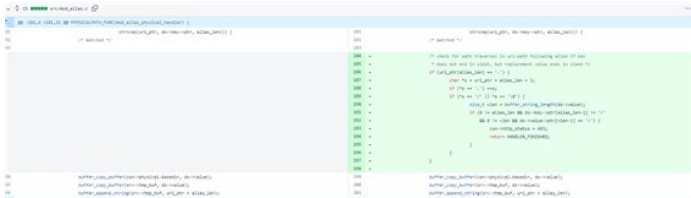


그림 9 CVE-2018-19052 보안성 개선 코드

4.2 CVE-2014-2323

소스 폴더 안에 mod_mysql_vhost.c 파일 안에 '와 같은 문자가 있으면 W'와 같이 이스케이프 처리해준다.



그림 10 CVE-2014-2323 보안성 개선 코드

5. 결 론

앞으로도 lighttpd 서버를 활용할 수 있는 분야는 무궁무진하다. 현재까지는 lighttpd에 대한 발견된 취약점이 많지 않지만 더 많은 곳에서 이 서버를 사용하게 되면 더 많은 취약점이 발생할 수 있기 때문에 해당 취약점에 대해 분석하고 해결 방법을 제시하였다. 위 방법을 시도해 공격자가 쉽게 정보를 탈취할 수 있다. 이에 대한 해결방법을 제시하여 위의 언급한 취약점들을 막을 수 있다. 하지만, 공격자는 또 다른 취약점을 찾기 위해 다양한 시도를 하고 정말 많은 공을 들인다. 그렇기 때문에 또 다른 취약점이 발생할 확률은 얼마든지 존재한다. 따라서 앞으로도 개발을 하고 배포를 하였다고 해도 끝이 아니고, 공격자의 마인드에서 어디가 취약할까 살펴보는 과정이 필요하고, 경각심을 가지고 끊임 없이 유지 보수 해야 한다.

참 고 문 헌

- [1] lighttpd – lighty labs,
<https://redmine.lighttpd.net/projects/lighttpd/wiki/>
- [2] lighttpd. <https://ko.wikipedia.org/wiki/Lighttpd>
- [3] Configure lighttpd alias (mod_alias).
https://www.cyberciti.biz/tips/configure-lighttpd-alias-mod_alias.html
- [4] CVE-2018-19052 Detail.
<https://nvd.nist.gov/vuln/detail/CVE-2018-19052>
- [5] CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').
<http://cwe.mitre.org/data/definitions/22.html>
- [6] CVE-2014-2323 Detail.
<https://nvd.nist.gov/vuln/detail/CVE-2014-2323>
- [7] CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').
<http://cwe.mitre.org/data/definitions/89.html>
- [8] Docs:ConfigurationOptions – lighttpd – Trac
<http://scm.zoomquiet.top/data/20070518123645/index.html>