

# 목차

|                                                                |   |
|----------------------------------------------------------------|---|
| <b>WAS 보안 취약점 점검</b> .....                                     | 3 |
| <b>서버 정보 노출</b> .....                                          | 3 |
| 원인 .....                                                       | 3 |
| 해결방법 .....                                                     | 3 |
| 참조링크 .....                                                     | 5 |
| <b>Directory Listing</b> .....                                 | 5 |
| <b>HTTP Method Limit</b> .....                                 | 6 |
| <b>AJP Secret</b> .....                                        | 6 |
| Tomcat .....                                                   | 7 |
| JBoss EAP 5.2.x .....                                          | 7 |
| JBoss EAP 6.4.x .....                                          | 7 |
| JBoss EAP 7.x .....                                            | 7 |
| mod_proxy (ajp를 사용하는 mod_proxy_ajp / mod_proxy_balancer) ..... | 8 |
| mod_jk .....                                                   | 8 |
| mod_cluster .....                                              | 8 |
| 관련링크 .....                                                     | 9 |

|            |      |                                                                                                                                                                                                                             |
|------------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last       | was_ |                                                                                                                                                                                                                             |
| update:    | 보    |                                                                                                                                                                                                                             |
| 2020/12/10 | 안    | <a href="https://atl.kr/dokuwiki/doku.php/was_%EB%B3%B4%EC%95%88_%EC%B7%A8%EC%95%BD%EC%A0%90_%EC%A0%90%EA%B2%80">https://atl.kr/dokuwiki/doku.php/was_%EB%B3%B4%EC%95%88_%EC%B7%A8%EC%95%BD%EC%A0%90_%EC%A0%90%EA%B2%80</a> |
| 03:30      | 취약   |                                                                                                                                                                                                                             |
|            | 점    |                                                                                                                                                                                                                             |
|            | 점검   |                                                                                                                                                                                                                             |

---

# WAS 보안 취약점 점검

## 서버 정보 노출

### 원인

서버 헤더에 해당 서버의 제품명, 버전등이 노출되는 문제

### 해결방법

#### Tomcat

server.xml 내의 connector 설정에 server 속성값을 추가한다. 또한 xpoweredBy="false"를 추가해준다. 다만 이 값은 false가 기본값이므로 없는 경우 굳이 추가할 필요는 없다.

```
<Connector port="8080" protocol="HTTP/1.1"
            connectionTimeout="20000"
            redirectPort="8443"
            server="bar"
            xpoweredBy="false"
            />
```

두번째 방법으로 X-Powered-By 헤더가 보이지 않게 하기 위해서는 web.xml내에 아래와 같은 내용을 추가하도록 한다.

단 이 방법은 아주 오래된 tomcat 6이전 버전에서 사용되던 방법으로 현재는 셋팅 해도 적용되지 않고 의미가 없는 설정이다.

```
<init-param>
    <param-name>xpoweredBy</param-name>
    <param-value>>false</param-value>
</init-param>
```

#### JBoss EAP 6.x

- SERVER 헤더

SERVER 헤더는 완전히 노출되지 않도록 할 수는 없습니다. 다만 헤더의 내용은 임의로 변경 가능합니다. 서버의 해당 org.apache.coyote.http11.Http11Protocol.SERVER Property값을 설정합니다.

```
org.apache.coyote.http11.Http11Protocol.SERVER="foo"
```

또는 설정파일내에 시스템 프로퍼티를 지정합니다.

```
<system-properties>
  <property name="org.apache.coyote.http11.Http11Protocol.SERVER"
value="foo"/>
</system-properties>
```

- X-PoweredBy 헤더

X-PoweredBy 헤더는 JBoss 옵션을 변경하도록 합니다.

```
/subsystem=web/configuration=jsp-configuration/:write-attribute(name=x-
powered-by,value=false)
{
  "outcome" => "success",
  "response-headers" => {
    "operation-requires-reload" => true,
    "process-state" => "reload-required"
  }
}
```

그러면 구성파일이 변경되고 아래 섹션이 추가됩니다.

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-
host" native="false">
  <configuration>
    <jsp-configuration x-powered-by="false"/>
  </configuration>
  ...
  ...
</subsystem>
```

서버를 다시 시작하고 변경 사항을 테스트하십시오.

## JBoss EAP 7.x

- Server: JBoss-EAP/7 와 X-Powered-By: Undertow/1 헤더

위 두 헤더 내용을 출력하지 않게 하려면 아래와같은 CLI명령어를 수행하도록 합니다.

```
/subsystem=undertow/server=default-server/host=default-host/filter-ref=x-
```

```
powered-by-header: remove
/subsystem=undertow/server=default-server/host=default-host/filter-
ref=server-header: remove
```

위 두 헤더를 다른 값으로 변경하고자 할 때는 아래 CLI명령어를 수행합니다.

```
/subsystem=undertow/configuration=filter/response-header=server-
header:write-attribute(name=header-value,value=foo)
/subsystem=undertow/configuration=filter/response-header=x-powered-by-
header:write-attribute(name=header-value,value=bar)
```

- X-Powered-By: JSP/2.3 헤더

이 헤더를 출력하지 않게 하려면 아래 CLI명령어를 수행합니다.

```
/subsystem=undertow/servlet-container=default/setting=jsp:write-
attribute(name=x-powered-by,value=false)
```

## 참조링크

- <https://access.redhat.com/solutions/21075>
- <https://tomcat.apache.org/tomcat-8.0-doc/security-howto.html#Connectors>
- <https://access.redhat.com/solutions/2740891>

## Directory Listing

기본적으로 디렉토리 내의 파일 목록이 출력되는것 방지하기

### Tomcat

- <https://tomcat.apache.org/tomcat-9.0-doc/default-servlet.html>

Tomcat 9 버전은 기본적으로 해당 기능이 비활성화 되어있다. 명시적으로 적용하기 위해서는 web.xml 내에 아래와 같이 listings 속성을 false로 지정하면 된다.

```
<servlet>
  <servlet-name>default</servlet-name>
  <servlet-class>
    org.apache.catalina.servlets.DefaultServlet
  </servlet-class>
  <init-param>
    <param-name>debug</param-name>
    <param-value>0</param-value>
  </init-param>
```

```
<init-param>
  <param-name>listings</param-name>
  <param-value>false</param-value>
</init-param>
<load-on-startup>1</load-on-startup>
</servlet>
```

## HTTP Method Limit

특정 HTTP Method를 제한 한다.

### Tomcat

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Protected Context</web-resource-name>
    <url-pattern>/*</url-pattern>
    <http-method>PUT</http-method>
    <http-method>DELETE</http-method>
    <http-method>HEAD</http-method>
    <http-method>TRACE</http-method>
    <http-method>OPTIONS</http-method>
  </web-resource-collection>
  <auth-constraint />
</security-constraint>
```

## AJP Secret

이것은 Tomcat / Undertow에서 AJP 프로토콜의 구성 문제입니다. AJP는 매우 신뢰할 수있는 프로토콜이므로 신뢰할 수없는 클라이언트에게 노출되어서는 안됩니다. 안전하지 않은 (일반 텍스트 전송) 네트워크가 안전하다고 가정합니다. AJP가 노출되지 않는 구성을 사용하여 예방 조치를 취해야 합니다.

우선 순위에 따라 다음 완화 조치 중 하나를 적용해야 합니다.

- Tomcat에서 AJP를 모두 비활성화하고 대신 프록시 연결에 HTTP 또는 HTTPS를 사용하십시오. HTTP 및 HTTPS에는 AJP와 동일한 신뢰 문제가 없습니다.
- 신뢰할 수 있는 호스트에서만 들어오는 연결이 허용되도록 네트워크 바인딩 및 방화벽 구성을 신중하게 검토 할뿐만 아니라 비밀로 AJP 연결을 보호하십시오.
- 네트워크 바인딩 및 방화벽 구성 만 사용하여 들어오는 연결이 신뢰할 수 있는 호스트에서만 허용 되도록하십시오.

첫 번째 옵션 인 AJP 비활성화는 가장 안전하고 강력한 권장 솔루션입니다. 비밀로 AJP를 보호하는 것은 덜 방해가 될 수 있지만 secret 매개 변수 를 지원 하는 httpd mod\_jk 버전 중 하나 를 사용해야 합니다 . 이 매개 변수는 현재 httpdRed Hat Enterprise Linux 7 및 8 버전에서 지원되지만 Red Hat Software

Collections에 포함 된 버전은이 매개 변수를 지원하지 않으므로 다른 완화 전략을 사용해야 합니다.

## Tomcat

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
address="YOUR_TOMCAT_IP_ADDRESS" requiredSecret="YOUR_AJP_SECRET" />
```

## JBoss EAP 5.2.x

```
<Connector protocol="AJP/1.3" port="8009" address="${jboss.bind.address}"
redirectPort="8443" requiredSecret="YOUR_AJP_SECRET"/>
```

## JBoss EAP 6.4.x

```
<system-properties>
  <property name="org.apache.coyote.ajp.DEFAULT_REQUIRED_SECRET"
value="YOUR_AJP_SECRET"/>
</system-properties>
```

## JBoss EAP 7.x

```
<subsystem xmlns="urn:jboss:domain:undertow:7.0" ...>
  ...
  <server name="default-server">
    <http-listener name="default" socket-binding="http" redirect-
socket="https" enable-http2="true"/>
    <ajp-listener name="ajp" socket-binding="ajp"/>
    <https-listener name="https" socket-binding="https" security-
realm="ApplicationRealm" enable-http2="true"/>
    <host name="default-host" alias="localhost">
      ...
      <!-- add the following with your AJP port (8009) -->
      <filter-ref name="secret-checker" predicate="equals(%p, 8009)"/>
    </host>
  </server>
  ...
  <filters>
    <!-- add the following with your credential (YOUR_AJP_SECRET) -->
    <expression-filter name="secret-checker" expression="not
equals(%{r,secret}, 'YOUR_AJP_SECRET') -> response-code(403)"/>
  </filters>
</subsystem>
```

```
/subsystem=undertow/configuration=filter/expression-filter=secret-
```

```
checker:add(expression="not equals(%{r,secret}, 'YOUR_AJP_SECRET') ->
response-code(403)")
/subsystem=undertow/server=default-server/host=default-host/filter-
ref=secret-checker:add(predicate="equals(%p,8009)")
```

## mod\_proxy (ajp를 사용하는 mod\_proxy\_ajp / mod\_proxy\_balancer)

이 secret특성은 다음 버전부터 지원됩니다. JBCS httpd 2.4.37; RHEL 7 httpd-2.4.6-67; RHEL 8 httpd-2.4.6-62

- mod\_proxy\_ajp의 경우 ProxyPass설정 의 secret속성을 추가 할 수 있습니다.
- mod\_proxy\_balancer의 경우 BalancerMember설정 의 secret속성을 추가 할 수 있습니다.

예를 들어 다음과 같이 secret=YOUR\_AJP\_SECRET구성을 추가 하십시오 (예 :  
<HTTPD\_HOME>/conf/httpd.conf또는 <HTTPD\_HOME>/conf.d/proxy\_ajp.conf).

- mod\_proxy\_ajp:

```
ProxyPass /example/ ajp://localhost:8009/example/ secret=YOUR_AJP_SECRET
```

- mod\_proxy\_balancer:

```
<Proxy balancer://mycluster>
    BalancerMember ajp://node1:8009 route=node1 secret=YOUR_AJP_SECRET
    BalancerMember ajp://node2:8009 route=node2 secret=YOUR_AJP_SECRET
</Proxy>
ProxyPass /example/ balancer://mycluster/example/
stickysession=JSESSIONID|jsessionid
```

## mod\_jk

- mod\_jk - workers.properties내에 worker 또는 loadbalancer 에 secret 속성을 지정할 수 있습니다. 로드 밸런서에서 secret을 설정하면 모든 구성원이 이 속성을 상속합니다. 이 secret속성 지원은 mod\_jk 1.2.12부터 추가되었습니다.

```
worker.<WORKER_NAME>.secret=YOUR_AJP_SECRET
```

## mod\_cluster

mod\_cluster 는 secret 속성을 지원하지 않습니다. mod\_cluster가 필요한 경우 Tomcat/JBoss 측의 AJP 커넥터에 구성된 경우 올바른 secret 연결할 수 없기 때문에 http또는 https대신 사용하도록 구성을 변경해야 합니다.

## 관련링크

- <https://access.redhat.com/solutions/4851251>

From:

<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:

[https://atl.kr/dokuwiki/doku.php/was\\_%EB%B3%B4%EC%95%88\\_%EC%B7%A8%EC%95%BD%EC%A0%90\\_%EC%A0%90%EA%B2%80](https://atl.kr/dokuwiki/doku.php/was_%EB%B3%B4%EC%95%88_%EC%B7%A8%EC%95%BD%EC%A0%90_%EC%A0%90%EA%B2%80)

Last update: 2020/12/10 03:30

