Company Name, Inc. Project name

보안대책-WAS
보안가이드라인

2017-04-19

오픈나루

Table of Contents

1. 개요

1.1 목적

본 문서는 'KISA 의 취약점 분석 · 평가 모델, CSI 의 IPAK 등 국내/외 위험분석 모델'에 의거한 점검 항목 및 보안 대책을 다루고 있으며, 정보 시스템 담당자의 취약점 이해 및 취약점 조치를 위한 보안 가이드를 제시하고자 한다.

주의사항
본 보안가이드 라인에서 제시하는 취약점 조치 방안은 일반적인 기술적 해결방안을 명시하고 있으며, 해당 OS·장비별 특성 등을 모두 반영하지 못한 실정입니다.

따라서,
취약점 조치 전 OS 벤더사, 담당운영자, APP 담당자 등과 사전 협의 후 조치하시기 바랍니다.

1.2 WAS 점검 항목

진단항목	TOMCAT	JBOSS
WS-01. 관리자 콘솔 관리	●	●
WS-02. 관리자 계정명 변경	●	●
WS-03. 관리자 패스워드 관리	●	●
WS-04. 패스워드 파일 관리	●	●
WS-05. 디렉토리 쓰기 권한 관리	●	●
WS-06. 소스/설정파일 권한 관리	●	●
WS-07. 디렉토리 검색 기능 제거	●	●
WS-08. 로깅 디렉토리/파일 권한 관리	●	●
WS-09. 에러 메시지 관리	●	●
WS-10. Sample Domain 삭제	●	●
WS-11. 최신 패치 적용	●	●

2. WAS 보안 가이드 라인

2.1 접근 제어

WS-01. 관리자 콘솔 관리

▶ 개요

- **취약점 설명**
  관리자 인증을 위한 페이지가 쉽게 인지 가능하거나 유추로 인해 접근되어지는 경우 Web 에 관련된 모든 권한을 누출할 수 있으므로 관리에 주의하여야 함
- **위험도 : 상**
- **점검기준**
  - 양호 : 관리자 콘솔을 사용하지 않고 사용 시 디폴트 포트로 접근이 불가능할 경우
  - 취약 : 관리자 콘솔을 사용하고 디폴트 포트로 접근이 가능한 경우
- **영향도**
  - TOMCAT : 관리자 콘솔의 접근 권한 설정은 서비스에 영향 없음
  - JBOSS : 관리자 콘솔의 접근 권한 설정은 서비스에 영향 없음

  관리자 콘솔 필요성에 대하여 확인 후 조치한다면 서비스 영향은 없으나 취약점 조치 시 WAS 운영자 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

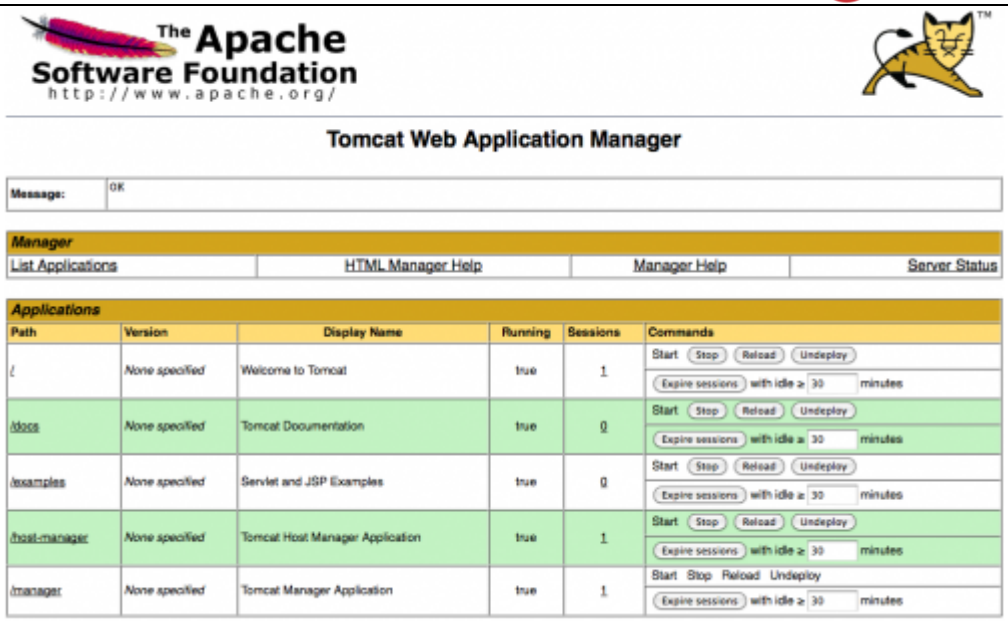
- **TOMCAT**

  ■ **확인방법**

  - Tomcat 관리자 콘솔 사용 유무 확인함

    예) http://[Domain]/manager/, http://[Domain]/admin/

    단, Tomcat 5.5.x 의 버전인 경우 admin 을 따로 다운로드를 받아 설치하여야 함


The Apache Software Foundation
http://www.apache.org/

Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

- 일반 사용자가 볼 수 없도록 접근경로에서 분리되어야 함

■ 조치방법

- 관리자 콘솔에서 콘솔 운영 관련 항목을 사용 금지하거나, 사용 시 Default 포트인 8080 은 공격자가 유추할 수 있으므로 유추할 수 없는 포트로 변경함

  권장 포트 범위 : 1024 ~ 65534

  설정 파일 : /[Tomcat Dir]/conf/server.xml

```
<Connector port="8080"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" redirectPort="8443" acceptCount="100"
           debug="0" connectionTimeout="20000"
           disableUploadTimeout="true" />
```

- 필요시에만 관리자 콘솔 운영을 권고함

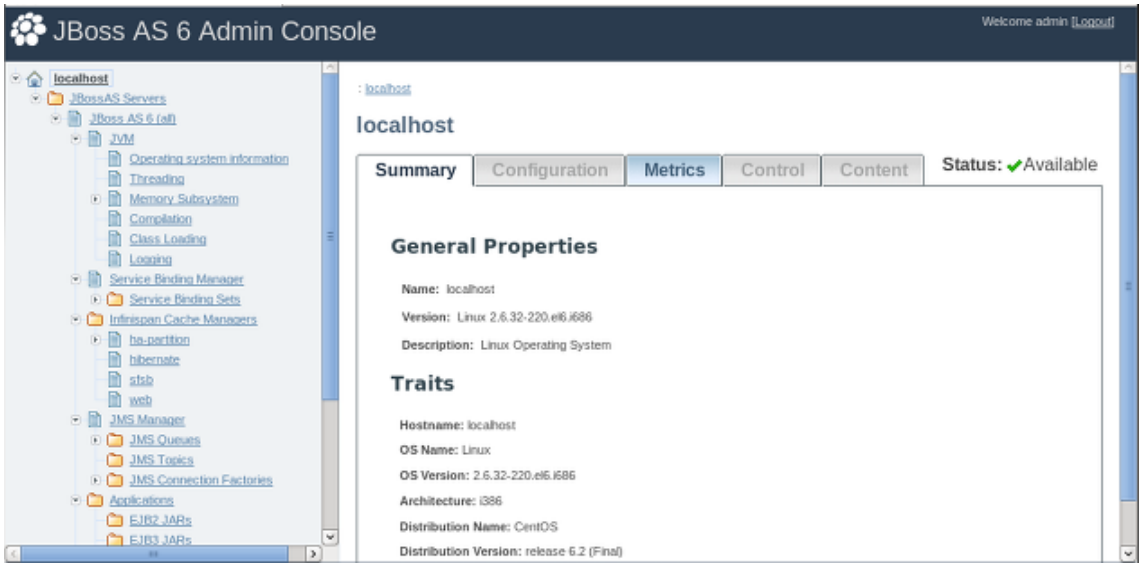
  필요한 경우에 한하여 관리자 콘솔을 사용하고 불필요한 경우 프로세스 종료

- **JBOSS**

■ **확인방법**

- JBOSS 관리자 콘솔 사용 유무 확인함

  예) http://[Domain]/manager/, http://[Domain]/admin-console/



■ **조치방법**

- 관리자 콘솔에서 콘솔 운영 관련 항목을 사용 금지하거나, 사용 시 Default 포트인 8080 은 공격자가 유추할 수 있으므로 유추할 수 없는 포트로 변경함

  권장 포트 범위 : 1024 ~ 65534

  설정 파일 : /[JBOSS Dir]/conf/server.xml

```
<Connector protocol="HTTP/1.1" port="8080"
  address="${jboss.bind.address}"
            connectionTimeout="20000" redirectPort="8443"" />
```

- 필요시에만 관리자 콘솔 운영을 권고함
  필요한 경우에 한하여 관리자 콘솔을 사용하고 불필요한 경우 프로세스 종료

WS-02. 관리자 계정명 변경

▶ 개요

- **취약점 설명**
  WAS 설치 시 web 관리자 콘솔 계정으로 Default 값인 Tomcat[admin]을 사용하는 경우가 존재함
  만일 , Default 값을 그대로 사용하는 경우 패스워드 유추 공격의 위험에 노출되므로, 타인이 유추하기 불가능한 계정명으로 변경 권고함
- **위험도 : 하**
- **점검기준**
  - 양호 : 계정명이 Default 계정으로 설정되어 있는 경우
  - 취약 : 계정명이 Default 계정으로 설정되어 있지 않은 경우
- **영향도**
  - TOMCAT : 계정 변경 후 boot/down 쉘에 계정명이 설정되어 있다면 변경 필요
  - JBOSS : 계정 변경 후 boot/down 쉘에 계정명이 설정되어 있다면 변경 필요

  관리자 계정명 변경에 대하여 취약점 조치 시 WAS 운영자 담당자와 협의하여 영향도 컴토 후 **단기 적용 필요**

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

  ■ **확인방법**

  - 관리자 콘솔 사용 시 User name 확인 및 변경
    설정파일 : /[Tomcat Dir]/conf/server.xml

  - 관리자 콘솔의 [User Definition] – [Users] – [Role Name]에서 계정명을 설정

  - Admin 계정과 일반 계정을 설정하여 줌 (default 계정 제외)

User	Password
tomcat	Tomcat

admin	설치 시 설정 값
both	Tomcat
Role 1	tomcat

■ **조치방법**

- 기본 유저와 패스워드를 삭제 또는 Roles 부분을 ""로 처리해 주어 기본 유저로의 로그인이 불가능 하도록 권고함

설정 파일 : /[Tomcat Dir]/conf/server.xml

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="shdusdk" description=""/>
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <role rolename="manager"/>
  <role rolename="admin"/>
  <user username="tomcat" password="tomcat"
   roles="admin,manager,tomcat"/>
  <user username="shdusdk" password="no9244" fullName="test"
   roles="admin,manager,tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
  </tomcat-users>
```

- **JBOSS**

■ **확인방법**

- 관리자 콘솔 사용 시 User name 확인 및 변경

설정파일

```
# cat /[JBOSS Dir]/server/default/deploy/management/console-mgr.sar/ ₩
web-console.war/WEB-INF/classes/web-console-users.properties
# A sample users.properties file for use with the UsersRolesLoginModule
```

admin=admin

- 관리자 패스워드 확인
- 관리자 패스워드 선정 시 다음 규칙에 따라 설정해야 함
  영수혼용 8 자 이상, 동일 문자 연속 5 회 이상 사용 금지
  계정 명과 동일하거나 패스워드 설정이 되어있지 않은 경우, 패스워드 변경

■ **조치방법**

- 관리자 계정/패스워드 변경
  기본 유저와 패스워드를 삭제 또는 Role 부분을 ""로 처리해 주어 기본 유저로의 로그인이 불가능 하도록 권고함

```
# cat /[JBOSS Dir]/server/default/deploy/management/console-mgr.sar/ ₩
  web-console.war/WEB-INF/classes/web-console-users.properties
# A sample users.properties file for use with the UsersRolesLoginModule
  admin=admin
```

WS-03. 관리자 패스워드 관리

▶ **개요**

- **취약점 설명**
  관리자 계정의 패스워드를 취약하게 설정하여 사용하는 경우, 비인가 사용자가 패스워드 유추 공격을 시도하여, 관리자 권한을 획득할 수 있음
- **위험도 : 중**
- **점검기준**
  - 양호 : 관리자 패스워드가 암호화 되어 있거나, 유추하기 쉬운 패스워드로 설정되어 있지 않을 경우
  - 취약 : 관리자 패스워드가 암호화 되어 있지 않거나 유추하기 쉬운 패스워드로 설정되어 있는 경우
- **영향도**
  - TOMCAT : 계정 변경 후 boot/down 쉘에 계정명이 설정되어 있다면 변경 필요
  - JBOSS : 계정 변경 후 boot/down 쉘에 계정명이 설정되어 있다면 변경 필요

일반적으로 서비스에 영향은 없으므로 **단기 적용** 가능

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ **확인방법**

- 관리자 패스워드를 암호화 하거나, 영/숫자/특수문자를 혼용하여 9 자리 이상 사용하도록 설정함

관리자가 패스워드 선정 시 다음 규칙에 따라 설정해야 함

영수혼용 9 자 이상, 동일문자 연속 5 회 이상 사용 금지
계정명과 동일하거나 패스워드 설정이 되어있지 않은 경우 패스워드 변경

■ **조치방법**

- 기본 유저와 패스워드를 삭제 또는 Roles 부분을 ""로 처리해 주어 기본 유저로의 로그인이 불가능 하도록 권고함

설정 파일 : /[Tomcat Dir]/conf/server.xml

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="shdusdk" description=""/>
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <role rolename="manager"/>
  <role rolename="admin"/>
  <user username="tomcat" password="tomcat"
   roles="admin,manager,tomcat"/>
  <user username="shdusdk" password="no9244" fullName="test"
   roles="admin,manager,tomcat"/>
```

```
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
```

- **JBOSS**

■ 확인방법

- 패스워드 파일의 권한 확인함

설정파일 : jmx-console-users.properties

■ 조치방법

- 관리자 패스워드를 암호화 하거나, 영/숫자/특수문자를 혼용하여 9 자리 이상 사용하도록 설정함

관리자가 패스워드 선정 시 다음 규칙에 따라 설정해야 함

영수혼용 9 자 이상, 동일 문자 5 회 이상 사용 금지
계정명과 동일하거나 패스워드 설정이 되어있지 않은 경우 패스워드 변경

- # vi jmx-console-users.prolerties

```
# A sample users.prolerties file for use with the UsersRolesLoginModule
admin=[변경할 패스워드]
```

WS-04. 패스워드 파일 관리

▶ 개요

- **취약점 설명**

- Tomcat

관리자 콘솔용 패스워드, 파일, Role 파일의 default 퍼미션이 644(rw-r—r--)로 설정되어 있다면 일반 사용자에게 패스워드가 노출될 수 있음
이 파일 내에는 계정과 패스워드가 평문으로 저장되어 있어 일반 계정이 읽을 경우, 관리 콘솔용 패스워드가 쉽게 노출될 수 있음

- **위험도 : 상**
- **점검기준**

- 양호 : 패스워드 파일에 권한이 640(rw-r-----) 이하로 설정되어 있을 경우
- 취약 : 패스워드 파일에 권한이 640(rw-r-----) 이하로 설정되어 있지 않을 경우

- **영향도**

실행 계정만 해당 파일에 접근 가능하다면 서비스에 영향 없으므로 **단기 적용** 가능

▶ **대상 S/W**

TOMCAT	JBOSS
●	●

▶ **조치 방안**

- **TOMCAT**

■ **확인방법**

- 패스워드 파일의 권환 확인함

설정 파일 : /[Tomcat Dir]/conf/tomcat-users.xml

■ **조치방법**

<Windows 환경>

- 패스워드 파일

Administrators 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 패스워드 파일 : 전용 WAS 계정 소유이고, 640(rw-r-----)이하 권한

- **JBOSS**

■ **확인방법**

- 패스워드 파일의 권한 확인함

설정파일 : jmx-console-users.properties

■ **조치방법**

<Windows 환경>

- 패스워드 파일

  Administrators 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 패스워드 파일 : 전용 WAS 계정 소유이고, 640(rw-r-----)이하 권한

2.2 설정

WS-05. 디렉토리 쓰기 권한 관리

▶ 개요

- **취약점 설명**
  일반 사용자가 웹 서버 홈 디렉토리 또는 설정관리 서버 디렉토리 및 매니지드 구동서버 디렉토리에 임의의 파일을 생성, 삭제 및 변경 할 경우, 홈페이지 변조, 중요파일 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있음
- **위험도 : 상**
- **점검기준**
  - 양호 : 홈 디렉토리 또는 웹 서버, 관리 서버 디렉터리 권한이 755(drwxr-xr-x)로 설정되어 있는 경우
  - 취약 : 홈 디렉터리 또는 웹 서버, 관리 서버 디렉터리 권한이 755(drwxr-xr-x)로 설정되어 있지 않은 경우
- **영향도**
  WAS 실행 계정만 해당 설정 파일 디렉토리에 접근 가능 하다면 서비스에 영향에 없으며, 소스 파일 디렉토리에는 타 계정에서 읽고/쓰기를 할 수 있으므로 확인 후 적용 필요 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여 영향도 검토 후 **증기 적용** 필요

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ **확인방법**

- 디렉토리 쓰기 권한을 확인함

웹 서버 홈 디렉토리

/[Tomcat 설치 디렉토리]/conf/server.xml(appBase 확인)

```
<Host  name="localhost" appBase="webapps"
        unpackWARs="true" autoDeploy="true"
        xmlValidation="false" xmlNamespaceAware="false">
```

관리 서버 홈 디렉토리

/[Tomcat Dir]/webapps/manage/

■ **조치방법**

<Windows 환경>

- 웹 서버 홈디렉토리

Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

- 관리 서버 홈디렉토리

Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 웹 서버 홈디렉토리

전용 WAS 계정 소유이고, 755(rwxr-xr-x)이하 권한

- 관리 서버 홈디렉토리

전용 WAS 계정 소유이고, 755(rwxr-xr-x)이하 권한

※ 파일 업로드 폴더가 있다면 쓰기 권한 부여

- **JBOSS**

■ 확인방법

- 디렉터리 쓰기 권한을 확인함

웹 서버 홈 디렉터리

/[JBOSS 설치 디렉터리]/conf/server.xml(appBase 확인)

```
<Host name = "localhost" appBase="webapps"
        unpackWARs="true" autoDeploy="true"
        xmlValidation="false" xmlNamespaceAware="false">
```

관리 서버 홈 디렉터리

/[JBOSS Dir]/webapps/manage/

■ 조치방법

<Windows 환경>

- 웹 서버 홈 디렉터리

Administrators 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

- 관리 서버 홈 디렉토리

Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 웹 서버 홈 디렉토리

전용 WAS 계정 소유이고, 755(rwxr—r--)이하 권한

- 관리 서버 홈 디렉토리

전용 WAS 계정 소유이고, 755(rwxr—r--)이하 권한

※ 파일 업로드 폴더가 있다면 쓰기 권한 부여

WS-06. 소스/설정파일 권한 관리

▶ 개요

- **취약점 설명**
  일반 사용자가 웹 사이트 소스파일을 삭제, 변경할 수 있으면, 홈페이지 변조,작업 실수로 인한 파일 삭제 , 백도어 삽입 등의 피해가 발생할 수 있음
  이로 인해 시스템이 오작동하여 사용 불능 상태에 빠질 우려가 있음
- **위험도 : 상**
- **점검기준**
  - 양호 : WAS 전용계정 소유이고 소스파일 퍼미션 644(rw-r—r--), 설정 파일 퍼미션 640(rw-r-----) 으로 설정되어 있는 경우
  - 취약 : WAS 전용계정 소유이고 소스파일 퍼미션 644(rw-r—r--), 설정파일 퍼미션 640(rw-r-----) 으로 설정되어 있지 않는 경우
- **영향도**
  소스 및 설정 파일은 WAS 실행 계정만 접근 가능 하다면 서비스에 영향은 없으나 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여 영향도 검토 후 **증기 적용** 필요

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ 확인방법

- 파일의 쓰기 권한 점검 확인

소스 파일

/[Tomcat 설치 디렉토리]/conf/server.xml(appBase 확인)

설정 파일

/[Tomcat 설치 디렉토리]/conf/ (해당파일: *.xml,*.properties,*.policy)

■ **조치방법**

<Windows 환경>

- 소스 파일

  Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

- 설정 파일

  Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 소스 파일

  전용 WAS 계정 소유이고, 644(rw-r--r--)이하 권한

- 설정 파일

  전용 WAS 계정 소유이고, 640(rw-r-----)또는 740(rwxr-----)이하 권한

- **JBOSS**

■ **확인방법**

- 파일의 쓰기 권한 점검 확인

  소스 파일

  /[JBOSS 설치 디렉터리]/conf/server.xml(appBase 확인)

  설정파일

  /[JBOSS 설치 디렉터리]/conf/(해당파일 : *.xml,*.properties, *.policy)

■ **조치방법**

<Windows 환경>

- 소스 파일

  Administrators 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

- 설정 파일

  Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(그룹 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 소스 파일

  전용 WAS 계정 소유이고, 644(rw-r—r--)이하 권한

- 설정 파일

  전용 WAS 계정 소유이고, 640(rw-r—r--) 또는 740(rwxr-----)

WS-07. 디렉토리 검색 기능 제거

▶ 개요

- **취약점 설명**
  디렉토리 검색 기능(Directory Indexing)이 설정되어 있는 경우, Web 서버 구조 노출 및 설치 파일의 유출 가능성이 있음
- **위험도 : 하**
- **점검기준**
  - 양호 : 디렉토리 검색 기능(Directory Indexing)이 설정되어 있지 않은 경우
  - 취약 : 디렉토리 검색 기능(Directory Indexing)이 설정되어 있는 경우
- **영향도**
  일반적인 경우 서비스에 영향은 없으나 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여 영향도 검토 후 **단기 적용** 가능

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ **조치 방안**

- **TOMCAT**

■ **확인방법**

- 해당 설정파일에서 false 인지 확인

설정 파일 : /[Tomcat 설치 디렉토리]/conf/web.xml

설정파일에서 <parapm-value>가 true 일 경우

```
- <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>
```

■ **조치방법**

- 해당 설정파일에서 false 로 조치 권고

설정 파일

/[Tomcat Dir]/conf/web.xml (<param-value>값 확인)

- **JBOSS**

■ **확인방법**

- 설정파일

/[JBOSS Dir]/WEB-INF/web.xml (<param-value>값 확인)에서 해당 설정파일에서 false 인지 확인

- 설정 파일에서 <param-value>가 true 일 경우

```
- <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>
```

■ **조치방법**

- 설정파일

  /[JBOSS Dir]/WEB-INF/web.xml 해당 설정파일에서 <param-value> 값이 false 로 조치 권고

WS-08. 로깅 디렉토리/파일 권한 관리

▶ 개요

- **취약점 설명**
  로그 파일에는 공격자에게 유용한 정보가 들어있을 수 있으므로 권한 관리가 필요함
  일반 사용자에 의한 정보 유출이 불가능 하도록 권한 설정을 강화함
- **위험도 : 중**
- **점검기준**
  - 양호 : Log 디렉토리의 퍼미션이 750(drwxr※--),로그파일 퍼미션이 650(rw-r---)이하일 경우
  - 취약 : Log 디렉토리의 퍼미션이 750,로그파일 퍼미션이 650 이하가 아닐 경우
- **영향도**
  타 계정에서 로그 디렉토리 및 로그 파일을 접근해야 하는지 확인이 필요하며 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여 영향도 검토 후 **단기 적용** 가능

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ **확인방법**

- Default 로그 디렉토리

/[Tomcat Dir]/logs/

■ **조치방법**

<Windows 환경>

- 로그 디렉토리

Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(쓰기 권한 제거), Everyone 그룹(그룹 제거)

- 로그 파일

Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정 그룹(Administrator)(모든 권한),Users 그룹(쓰기 권한 제거), Everyone 그룹(그룹 제거)

<Unix 환경>

- 로그 디렉토리

전용 WAS 계정 소유이고, 750(drwxr-x---) 이하 권한

- 로그 파일

전용 WAS 계정 소유이고, 650(rw-r-x---) 이하 권한

- **JBOSS**

■ **확인방법**

- 로그 파일의 권한 점검

default 로그 디렉토리

/[JBOSS Dir]/logs/

■ **조치방법**

<Windows 환경>

- 로그 디렉토리

Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정

그룹(Administrator)(모든 권한),Users 그룹(쓰기 권한 제거),
Everyone 그룹(그룹 제거)

- 로그 파일
Administrator 또는 전용 WAS 계정 소유이고, 전용 WAS 계정
그룹(Administrator)(모든 권한),Users 그룹(쓰기 권한 제거),
Everyone 그룹(그룹 제거)

<Unix 환경>

- 로그 디렉토리
전용 WAS 계정 소유이고, 750(drwxr-x---) 이하 권한

- 로그 파일
전용 WAS 계정 소유이고, 650(rw-r-x---) 이하 권한

WS-09. 에러 메시지 관리

▶ 개요

- **취약점 설명**
공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 돌아오는 에러메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있음
- **위험도 : 중**
- **점검기준**
  - 양호 : 에러코드를 유추 불가능 하도록 일원화된 에러 메시지를 생성한 경우
  - 취약 : 에러코드를 유추 불가능 하도록 일원화된 에러 메시지를 생성하지 않은 경우
- **영향도**
일반적인 경우 서비스에 영향 없으며 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여 영향도 검토 후 **단기 적용** 가능
※ 사용자 브라우저로 에러 메시지 반환 여부 확인

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ 확인방법

- 설정파일 : /[Tomcat Dir]/conf/web.xml

■ 조치방법

- 사용자 브라우저로 에러 메시지 반환 여부 확인
- 설정파일에서 에러 메시지 설정 확인(필수 설정 : 400,401,403,404,500)
  설정파일 : /[Tomcat Dir]/conf/web.xml(error 메시지 처리 확인)

```
<welcome-file-list>
<welcome-file>index.html</welcome-file>
  <welcome-file>index.htm</welcome-file>
</welcome-file-list>
<error-page>
  <error-code>404</error-code>
  <location>/error.jsp</location>
</error-page>
<error-page>
  <error-code>500</error-code>
  <location>/error.jsp</location>
</error-page>
```

- **JBOSS**

■ 확인방법

/[JBOSS 설치 디렉터리]/conf/web.xml 에서 마지막 부분에 error 메시지 처리 부분이 있는지 확인

■ **조치방법**

에러 설정에서 많이 발생하는 에러코드에 대해서 에러페이지를 생성하여 해당 URL 로

이동시키도록 web.xml 파일에 해당 내용을 추가하여 조치

```
<welcome-file-list>
<welcome-file>index.html</welcome-file>
   <welcome-file>index.htm</welcome-file>
</welcome-file-list>
<error-page>
   <error-code>404</error-code>
   <location>/error.jsp</location>
</error-page>
<error-page>
   <error-code>500</error-code>
   <location>/error.jsp</location>
</error-page>
```

2.3 솔루션 취약점

WS-10. Sample domain 삭제

▶ **개요**

- **취약점 설명**
  솔루션 설치 시 기본적으로 제공되어 지는 sample 응용 프로그램들을 삭제 권고함
  이는 Sample 로 제공되는 예제 응용 프로그램들이 기동되어 서비스로 제공될 수 있으므로,
  제공되는 서비스를 제외한 나머지 응용프로그램들은 설치 제거 및 중지를 권고함
- **위험도 : 중**
- **점검기준**
  - 양호 : 불필요한 Sample/Example 디렉토리가 존재하지 않은 경우
  - 취약 : 불필요한 Sample/Example 디렉토리가 존재하는 경우
- **영향도**
  일반적인 경우 서비스에 영향 없으며 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여
  영향도 검토 후 **단기 적용** 가능

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ **확인방법**

- 해당 Example 디렉토리 삭제 여부 점검

설정파일 : /[Tomcat Dir]/webapps/examples/

■ **조치방법**

- Examples 설치 경로 확인 및 존재하면 삭제

설치 경로 : /[Tomcat Dir]/webapps/examples/

- **JBOSS**

■ **확인방법**

- 해당 Example 디렉토리 삭제 여부 점검

설정파일 : /[JBOSS Dir]/webapps/examples/

■ **조치방법**

- Examples 설치 경로 확인 및 존재하면 삭제

설치 경로 : /[JBOSS Dir]/webapps/examples/

2.4 보안 패치

WS-11. 최신 패치 적용

▶ 개요

- **취약점 설명**
  주기적으로 보안 패치를 적용하지 않으면 서버 침해가 발생할 수 있음
  최신의 버전과 패치를 확인 후 업그레이드 및 패치 수행
- **위험도 : 중**
- **점검기준**
  - 양호 : 최신 패치를 적용 하였을 경우
  - 취약 : 최신 패치를 적용 하지 않았을 경우
- **영향도**
  서비스 벤더를 통해 안정화 된 버전을 문의하여 적용 하여야 하며 취약점 조치 시 WAS 운영자 및 유지보수 담당자와 협의하여 영향도 검토 후 **중기 적용** 필요

▶ 대상 S/W

TOMCAT	JBOSS
●	●

▶ 조치 방안

- **TOMCAT**

■ **확인방법**

- 버전 확인 : /[Tomcat Dir]/bin/version.sh 확인

■ **조치방법**

- 최신 패치를 확인 후 업그레이드 및 패치 수행(최종 확인날짜 : 2017 년 4 월)

제품명	적용 패치
Tomcat 8.5.x	8.5.13
Tomcat 8.0.x	8.0.43
Tomcat 7.0.x	7.0.77
Tomcat 6.0.x	6.0.53

- **JBOSS**

■ 확인방법

- 버전 확인 : /[JBOSS Dir]/bin/run.sh 확인

```
# /[JBOSS Dir]/bin/run.sh | grep JBOSS_HOME,
```

■ 조치방법

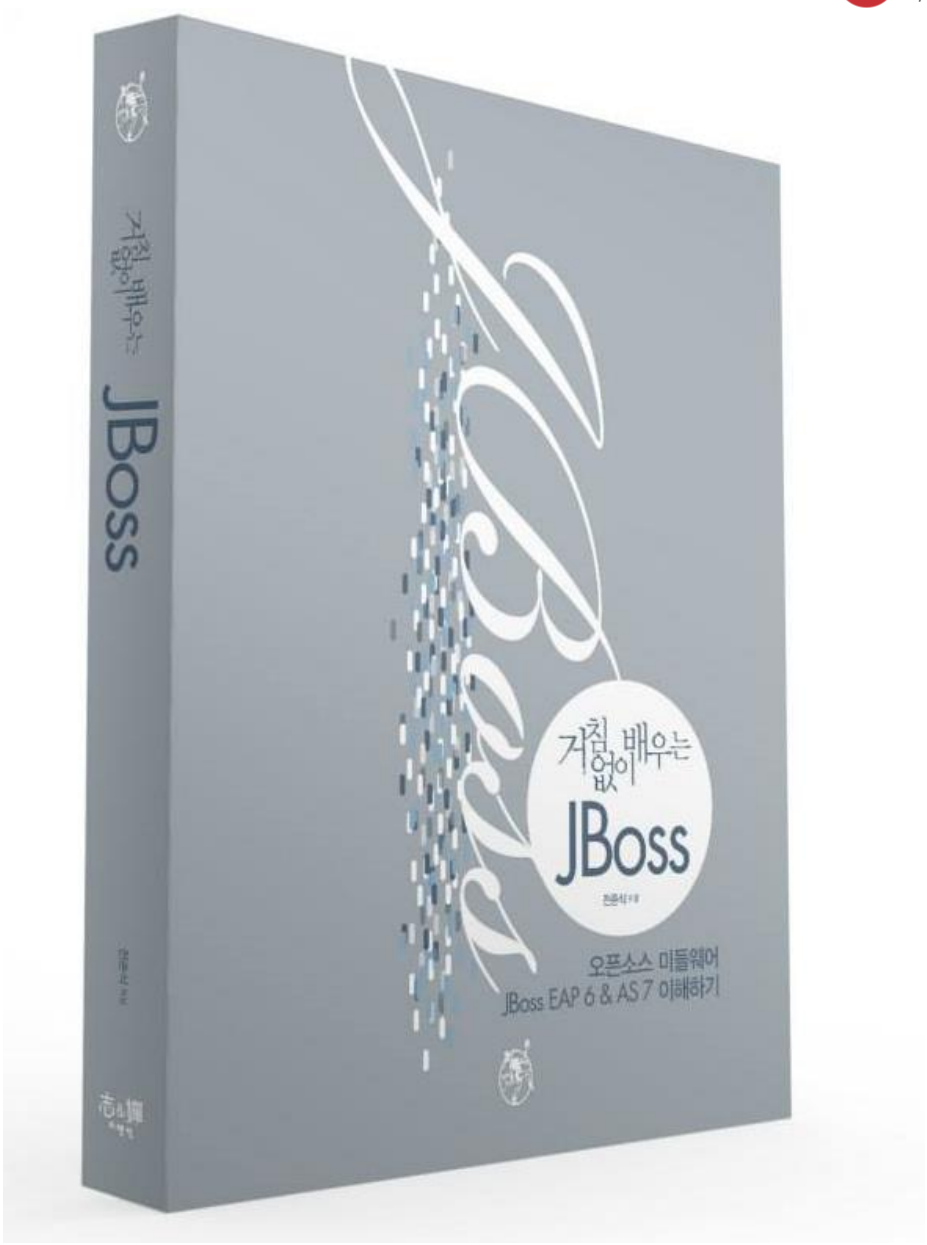
- 최신 패치를 확인 후 업그레이드 및 패치 수행(최종 확인날짜 : 2014 년 7 월)

제품명	적용 패치
EAP 6.3.0 Beta	EAP built from AS 7.4
EAP 6.3.0 Alpha	EAP built from AS 7.4
EAP 6.2.1 GA	EAP built from AS 7.3

※ 참고 사이트 : http://www.jboss.org/jbossas/downlods

3. 도움이 필요하십니까?

만약 이 문서에 설명된 절차를 수행할 때 문제를 겪는다면, 오픈나루 고객 포털(http://support.opennaru.com)을 방문하십시오.


거침없이 배우는
JBoss
오픈소스 미들웨어
JBoss EAP 6 & AS 7 이해하기

4. References

- **Red Hat Documentation**
  - http://docs.redhat.com/

- **Red Hat 고객지원 포탈**
  - http://access.redhat.com

- **오픈나루 고객지원 포탈**
  - http://support.opennaru.com

- **오픈나루 기술 Blog**
  - http://opennaru.tistory.com

- **오픈나루 Facebook Page**
  - https://www.facebook.com/opennaru

t : +82-2-469-5426 **f** : +82-2-469-7247

e : service@opennaru.com, sales@opennaru.com

h : http://www.opennaru.com