



<b>1. 계정관리 .....</b>	<b>5</b>
1.1. 관리자 페이지 관리.....	5
1.2. 관리자 계정명 변경.....	7
1.3. 관리자 패스워드 관리 .....	8
1.4. 패스워드 파일 관리.....	9
<b>2. 보안관리 .....</b>	<b>10</b>
2.1. 데몬 관리.....	10
2.2. 디렉토리 쓰기 권한 관리 .....	11
2.3. 소스/설정파일 권한 관리.....	12
2.4. 디렉토리 검색 기능 제거 .....	13
2.5. 에러 메시지 관리 .....	14
2.6. Examples 디렉토리 삭제.....	16
2.7. 프로세스 관리기능 삭제.....	17
<b>3. 로그 및 패치 관리 .....</b>	<b>18</b>
3.1. 로깅 디렉토리/파일 권한 관리 .....	18
3.2. 최신 패치 적용 .....	20

대상	Tomcat	위험도	상	code	WT-01
취약점 개요	Web환경에서 관리자 페이지를 제공하는 Tomcat Manager는 웹 브라우저의 주소란에서 직접 동작시킬 수 있는 간단한 Deploy 툴이다. 자바 클래스 등이 변경되거나 struts-config.xml과 같은 설정 파일이 변경되었을 때마다 tomcat을 재시작 해야 할 때 Tomcat Manager를 이용하면 좀 더 편하고 속도도 빨라진다. 하지만, 웹 브라우저를 통해서 웹서비스에 관련된 모든 권한의 제어가 가능하여 관리에 주의가 필요하고, 관리자 인증 페이지가 추측 가능하므로 노출되는 경우 웹서비스 연속성에 영향을 미칠 수 있다.				
<b>보안대책</b>					
판단기준	<b>양호:</b> 관리자 페이지에 접근제한이 설정되어 있는 경우 <b>취약:</b> 관리자 페이지에 접근제한이 설정되어 있지 않은 경우				
조치방법	관리자 페이지에 접근제한 설정				
<b>보안설정방법</b>					

대상	Tomcat	위험도	상	code	WT-02
<b>취약점 개요</b>	Tomcat 에서 admin tools을 설치하여 사용할 경우 default 값으로 제공된 계정의 사용을 중지하고 유추하기 힘든 새로운 사용자 계정을 추가하고 권한을 설정 후 사용할 것을 권고. Default 계정을 그대로 사용하는 경우, [brute-force] 공격의 위험에 노출되는 취약점이 존재하므로 타 유추 불가능한 계정명으로 변경 권고함.				
<b>보안대책</b>					
<b>판단기준</b>	<b>양호:</b> Default 계정을 변경하여 사용하는 경우				
	<b>취약:</b> Default 계정을 변경하여 사용하지 않은 경우				
<b>조치방법</b>	관리자 콘솔 사용시 User name 확인 및 변경 관리자 콘솔의 [User Definition]-[Users]-[Role Name]에서 계정명을 설정.				

대상	Tomcat	위험도	상	code	WT-03
취약점 개요	<b>비인가 사용자에 의한 패스워드 유추 방지</b> 관리자 계정의 패스워드를 취약하게 설정하여 사용하는 경우, 비인가 사용자가 패스워드 유추, 공격을 시도하여, 관리자 권한을 획득할 수 있음. 3가지 조합 8글자 이상, 2가지 조합 10글자 이상				
<b>보안대책</b>					
판단기준	<b>양호:</b> 관리자 패스워드를 권고안대로 변경한 경우				
	<b>취약:</b> 관리자 패스워드를 권고안대로 변경하지 않은 경우				
조치방법	콘솔 상에서의 패스워드 변경 함. 관리자 콘솔 [Users]-[User Name]-[Password] 패스워드 설정.				

대상	Tomcat, OS(Windows, Unix)	위험도	상	code	WT-04
<b>취약점 개요</b>	관리자 콘솔용 패스워드 파일, Role 파일의 default 퍼미션이 644(rw-r--r--)로 설정되어 일반 사용자에게 노출될 수 있음. 이 파일내에는 계정과 패스워드가 평문으로 저장되어 있어 일반계정이 읽을 경우, 관리 콘솔용 패스워드 파일이 쉽게 노출됨				
<b>보안대책</b>					
<b>판단기준</b>	<b>양호:</b> 패스워드 파일을 각각의 OS에서 조치방안대로 권한을 준 경우				
	<b>취약:</b> 패스워드 파일을 각각의 OS에서 조치방안대로 권한을 주지 않은 경우				
<b>조치방법</b>	패스워드 파일의 권한 확인함. 설정파일 : /[Tomcat Dir]/conf/tomcat-users.xml				

대상	Tomcat, OS(Windows, Unix)	위험도	중	code	WT-05
<b>취약점 개요</b>	Tomcat 서버 데몬이 root 권한으로 운영되지 않도록 관리해야 함  WAS 서버 데몬이 root 권한으로 운영될 경우 WAS Application의 취약점이나  Buffer Overflow시 공격자에게 root권한을 유출할 수 있음.				
<b>보안대책</b>					
<b>판단기준</b>	<b>양호:</b> 서버 데몬이 root권한으로 운영하지 않는 경우  <b>취약:</b> 서버 데몬이 root권한으로 운영하는 경우				
<b>조치방법</b>	console에서 웹서버 서비스 구동상태 확인				
<b>보안설정방법</b>					

대상	Tomcat, OS(Windows, Unix)	위험도	중	code	WT-06
취약점 개요	<p><b>웹 사이트 변조 예방</b>            일반 사용자가 웹 서버 홈 디렉토리에 임의의 파일을 생성, 삭제, 변경할 수 있으면, 홈페이지 변조, 작업 실수로 인한 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있음</p>				
<b>보안대책</b>					
판단기준	<b>양호:</b> 디렉토리 쓰기 권한을 각각의 OS에서 조치방안대로 준 경우 <b>취약:</b> 디렉토리 쓰기 권한을 각각의 OS에서 조치방안대로 주지 않은 경우				
	<b>조치방법</b> 디렉토리 쓰기 권한을 확인				
<b>보안설정방법</b>					

대상	Tomcat, OS(Windows, Unix)	위험도	상	code	WT-07
취약점 개요	<p>비인가 사용자에 의한 소스 변경 예방            일반 사용자가 웹 사이트 소스 파일을 삭제, 변경할 수 있으면, 홈페이지 변조, 작업 실수로 인한 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있음            일반 사용자가 웹 서버의 설정 파일을 삭제, 변경할 수 있으면, 시스템이 오작동하여 사용 불능 상태에 빠질 우려가 있음.</p>				
<b>보안대책</b>					
판단기준	<p><b>양호:</b> 소스/설정파일 권한을 각각의 OS에서 조치방안대로 준 경우  <b>취약:</b> 소스/설정파일 권한을 각각의 OS에서 조치방안대로 주지 않은 경우</p>				
조치방법	파일의 쓰기 권한 점검 확인				
<b>보안설정방법</b>					

대상	Tomcat	위험도	상	code	WT-08
취약점 개요	디렉토리 검색 기능(Directory Indexing)이 설정되어 있는 경우, Web 서버 구조 노출 및 설치 파일의 유출 가능성이 있음. 디렉터리 검색은 웹 어플리케이션에 존재하는 파일목록을 보여주는 취약점이다. 디렉터리 요청 시 디렉터리 내에 존재하는 파일 목록을 보여주지 않도록 설정해야 한다. 디렉터리 내에 존재하는 DB 패스워드 파일이나 웹 어플리케이션 소스 코드 등 중요한 파일들에 대해 직접 접근이 가능하면 보안상 매우 위험하다. 이를 위해 디렉터리 검색 기능의 사용을 중지시킨다.				
<b>보안대책</b>					
판단기준	<b>양호:</b> 디렉터리 검색이 제한되어 있는 경우				
	<b>취약:</b> 디렉터리 검색이 제한되어 있지 않은 경우				
조치방법	해당 설정파일에서 false 인지 확인(default : false)				
<b>보안설정방법</b>					

대상	Tomcat, OS(Windows)	위험도	하	code	WT-09
<b>취약점 개요</b>	사용자의 실수 또는 고의적인 입력 데이터에 대해 웹 어플리케이션은 시스템 에러를 보이거나 특정 에러 페이지로 이동하는 등의 결과를 나타낸다. 이 중에서 시스템 에러 노출은 시스템 정보 제공으로 인해 웹 어플리케이션 스택 정보, 데이터베이스 주요정보 등의 내용이 에러 내용 중에 포함될 수 있어 공격자에게 잠재적인 취약점을 제공함으로써 시스템 운영을 저해할 수 있는 요소가 될 수 있다.				
<b>보안대책</b>					
<b>판단기준</b>	<b>양호:</b> 에러코드에 대한 별도의 에러 페이지가 설정된 경우 (에러 페이지 필수 설정 항목 : 400, 401, 403, 404, 500)				
	<b>취약:</b> 에러코드에 대한 별도의 에러 페이지가 설정되지 않은 경우				
<b>조치방법</b>	<b>사용자 브라우저로 에러 메시지 반환 여부 확인</b> <b>설정파일에서 에러 메시지 설정 확인</b> (필수 설정 : 400, 401, 403, 404, 500) 설정 파일 : /[Tomcat Dir]/conf/web.xml (error 메시지 처리 확인)				

대상	Tomcat	위험도	하	code	WT-10					
취약점 개요	불필요한 examples 디렉토리(/examples) 제거 서버에 대한 상세 정보를 제공하고 있고, 예제 프로그램 취약점 공격 예방을 위해서는 삭제하는 것이 바람직함.									
<b>보안대책</b>										
판단기준	<b>양호:</b> 불필요한 examples 디렉토리가 없을 경우 <b>취약:</b> 불필요한 examples 디렉토리가 있을 경우									
조치방법	Examples 디렉터리 삭제									
<b>보안설정방법</b>										
<p>■ <b>보안설정방법</b></p> <p>Examples 설치경로 확인 및 존재하면 삭제. 설치 경로 : /[Tomcat Dir]/webapps/examples/</p>										
조치 시 영향	일반적으로 영향 없음									

대상	Tomcat	위험도	중	code	WT-11
취약점 개요	해당 시스템의 관리자가 아닌, 일반 사용자가 프로세스 관리 페이지에 접속하여 통제 가능하여 진다면 시스템이 사용 불능 상태에 빠질 우려가 있음.				
<b>보안대책</b>					
판단기준	<b>양호:</b> 불필요한 examples 디렉토리가 없을 경우				
	<b>취약:</b> 불필요한 examples 디렉토리가 있을 경우				
조치방법	다음 경로가 프로세스 관리기능이 있는지 점검				
<b>보안설정방법</b>					

대상	Tomcat	위험도	상	code	WT-12
<b>취약점 개요</b>	로그 파일에는 공격자에게 유용한 정보가 들어있을 수 있으므로 권한 관리가 필요함. 일반 사용자에 의한 정보 유출이 불가능하도록 권한 설정을 강화함.				
<b>보안대책</b>					
<b>판단기준</b>	<b>양호:</b> 로그 디렉터리 및 파일(access Log, error Log)이 존재하는 경우 <b>취약:</b> 로그 디렉터리 및 파일(access Log, error Log)이 접근관리를 하는 경우				
<b>조치방법</b>	로그 디렉터리 및 파일의 권한 확인 및 변경				
<b>보안설정방법</b>					

대상	Tomcat	위험도	상	code	WT-13
취약점 개요	최신 보안패치가 적용되지 않을 경우 Tomcat 웹서버 취약점을 이용하여 서비스 거부(Dos)공격, 파일 업로드, 디렉터리 노출, 다중 확장자 처리 등 웹서비스에 직접적인 영향을 발생시키는 문제를 발생시키기 때문에 주기적인 보안 패치가 필요하다.				
보안대책					
판단기준	<b>양호:</b> 최신 보안패치가 적용되어 있는 경우				
	<b>취약:</b> 최신 보안패치가 적용되어 있지 않은 경우				
조치방법	최신 패치에 대한 현재 운영 영향도를 파악한 후 패치 여부 결정				
보안설정방법					