㈜아이티아이즈 보안취약점 점검지침은 클라우드 지원서비스를 제공하기 위한 운영문서로서 검토되고 승인됨	구분	직위	성명	일자	서명
	승인	클라우드서비스 최고책임자	조왕래		
	검토	클라우드서비스 관리자	김종룡		
	작성	클라우드서비스 담당자	김대회		

보안취약점 점검지침

2022.10.11

IT eyes Inc.

재•개정 이력사항				
번호	**날짜**	**쪽**	**내용**	**담당자**
1	2022.10.11	19	최초 보안취약점 점검지침 Ver1.0	김선환

본 문서는 ㈜아이티아이스 클라우드 서비스 제공을 위해서 컨설팅, 마이그레이션, 매니지드, XaaS 서비스 등을 대상으로 작성함.

제 1 장 총칙

제 1 조(목적)

본 지침은 ㈜ 아이티아이즈 (이하 “회사”라 함)의 클라우드 서비스 공공 정보시스템에 대한 주기적인 보안 점검을 수행함으로써 주요 자산의 위협에 대한 노출을 최소화하는데 그 목적이 있다.

제 2 조(적용범위)

본 지침은 모든 클라우드 서비스를 제공받는 고객의 정보시스템자산과 소프트웨어와 하드웨어, 네트워크를 대상으로 한다. 또한 정보시스템자산에 문제가 발생하거나 또는 발생할 수 있는 위협요인을 식별하여, 점검에 필요한 웹 취약점은 ‘안전행안부 취약점 항목’ 기준으로 점검항목으로 선정한다.

제 3 조(용어정의)

① 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. 취약점: 정보시스템자산 내에서 일반사용자가 권한 상승하여 관리자 권한을 획득하거나 비인가 외부자가 특정 권한을 획득할 수 있는 보안상의 결함을 의미한다. "개인정보 처리"란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂 正), 복구, 이용, 제공, 공개, 파기(破 棄), 그 밖에 이와 유사한 행위를 말한다.

2. 포트: 일반적으로 포트는 다른 장치에 물리적으로 접속되는 특정한 부위를 말하나, 네트워크에서는 인터넷이나 기타 다른 네트워크 메시지를 서버에 전달 혹은 도착하는 출입구를 의미한다.

3. 취약점점검: 정보시스템의 보안정책을 위반하기 위해 악용되는 시스템의 설계, 구현, 운영, 관리상의 취약점의 존재 여부를 확인하는 일련의 업무를 의미한다.

4. 취약점 점검도구: 보안 취약점 점검 기술 중의 한 분야로서 시스템 기반의 보안 취약점을 점검하는 기능을 가진 도구를 의미한다.

5. 가상화 : 가상화를 관리하는 소프트웨어(주로 Hypervisor)를 사용하여 하나의 물리적 머신에서 가상 머신(VM)을 만드는 프로세스이다.

6. 클라우드 : 인터넷을 통해 액세스할 수 있는 서버와 이러한 서버에서 작동하는 소프트웨어와 데이터베이스를

의미합니다.

7. 정보시스템 : 데이터를 입력받아 처리하여 정보를 산출하는 시스템이다.

8. 소프트웨어 : 컴퓨터에게 동작 방법을 지시하는 명령어 집합의 모임이다.

제 4 조(책임사항)

이 지침에서 운영관리하는 책임자와 담당자의 역할에 따른 책임사항 일체를 명기했습니다.

① 정보보호책임자 책임사항은

1. 정보시스템자산에 대하여 주기적(연 1 회 이상)으로 취약점 점검이 이루어지도록 수행 · 관리 · 감독을 수행한다.

2. 취약점 점검업무를 자체적으로 수행하기 어려운 경우 관련기관이나 외부 정보보호업체를 통해 지원을 받도록 한다.

② 정보보호관리자

1. 정보시스템자산에 대하여 주기적(연 1 회 이상)으로 취약점 점검이 이루어지도록 관리를 수행한다.

2. 점검결과는 정보보호책임자에게 보고하고 발견된 취약점은 제거하도록 조치한다.

③ 정보보호담당자

1. 정보시스템자산에 대하여 주기적(연 1 회 이상)으로 취약점 점검이 이루어지도록 점검을 수행한다.

2. 점검결과는 정보보호관리자에게 보고하고 발견된 취약점은 제거하도록 조치한다.

3. 서버, 네트워크, 정보보호시스템 등 정보시스템자산에 대하여 해당 담당자는 발견된 취약점을 제거할 의무를 갖는다.

제 2 장 웹 취약점 점검

제 5 조(웹 취약점 점검 대상)

① 웹 취약점 점검 시기

1. 웹 정보시스템의 취약점 점검은 매년 1 회 이상 진행하는 것을 원칙으로 한다.

② 취약점 점검 대상

1. 서버: 웹서버, WAS 서버, DB 서버, NC 서버 등의 서버

2. 정보보호시스템: UTM, 웹방화벽, 방화벽, IPS, IDS 등

3. DB : DBMS

4. PC(전사 자원 대상) : 노트북, 테블릿 PC 등

5. 웹서비스

제 6 조(웹 취약점검방법의 결정)

① 네트워크기반 취약점 점검: 시스템 취약점 분석 방법에는 자동화된 스캐닝 도구를 사용해 원격으로 점검하는 방법

② 시스템기반 취약점 점검 체크리스트 기반으로 로컬에서 점검하는 방법으로 구분할 수 있으며 외부 정보보호업체 등을 통하여 수행할 수도 있다.

③ 모의해킹은 애플리케이션 레벨 및 시스템의 취약점을 내부 보안 전문가의 모의해킹을 통해 파악한다. 외부 업체를 이용하여 진행할 수도 있다.

④ 취약점 점검도구의 이용은 특정한 소수의 취약점 탐지보다는 다수의 취약점 항목을 자동으로 점검할 수 있다.

제 7 조(웹 취약점 점검도구의 선정)

③ 취약점 정보, 취약점 데이터베이스, 신규 취약점 업데이트 기능, 취약점 점검결과의 정확성, 취약점 점검결과 보고서, 사용자의 편의성, 한글의 지원, 점검도구의 안정성을 고려하여 점검도구를 선정한다

제 8 조(웹 취약점 점검 도구)

① 네트워크 취약점 점검도구

1. Nessus 등

② 시스템 취약점 점검도구

1. LSOF(List Open File) 등

③ 공개 취약점 점검도구를 다운로드 받기 위해서는 다음 사이트를 참조한다.

1. http://www.krcert.or.kr 의 자료실 -> 보안도구 메뉴에서 다운

④ 기타 취약점 점검 도구: 아큐네틱스, 시큐아이스캔 등

제 9 조(웹 취약점 점검 도구 관리)

① 웹 취약점 점검도구의 사용 및 관리는 정보보호책임자로 제한한다.

② 정보보호책임자는 취약점 점검도구의 접근통제에 대한 관리책임을 지며, 새로운 취약점이 발견될 경우 취약점 점검도구의 취약점 데이터베이스에 대한 업데이트를 실시한다.

제 10 조(웹 취약점 점검항목의 선정)

① 정보시스템자산에 문제가 발생하거나 또는 발생할 수 있는 위협요인을 식별하여, 점검에 필요한 취약점은 '안전행안부 취약점 항목' 기준으로 점검항목으로 선정한다.

제 11 조(웹 취약점 점검의 수행)

① 침해사고대응팀은 분석.평가 시 발견된 미 준수 항목 및 정보보호 취약점을 평가한 후 취약점 분석.평가 결과를 취약점과 관련된 각 관리부서에 전달한다. 취약점 분석. 평가 결과에는 다음 각 항목의 내용이 포함되어야 한다.

1. 웹 취약점 분석 평가 수행 일시
2. 웹 취약점 분석 평가 대상
3. 웹 취약점 분석 방법
4. 웹 취약점 점검 내용 및 결과
5. 웹 취약점 조치 가이드 라인

제 12 조(발견된 취약점의 조치)

① 웹 취약점 점검을 통해 발견된 취약점에 대해서 적절한 조치와 해결책을 마련하도록 한다.

② 웹 취약점 점검결과에 대해 기존 정보보호대책의 적정성, 효율성 및 문제점을 평가하고 분석한다.

③ 정보보호대책(방침, 절차, 시스템) 등의 보완이 필요할 경우 기존 대책과 연계하여 효과성, 경제성을 바탕으로 가장 효율적인 대책과 추진방법을 선정한다.

④ 웹 취약점 조치가 완료되면 [첨부 1]웹 취약점 사후 조치보고서를 작성후 정보보호책임자에게 제출한다.

제 3 장 앱 취약점 점검

제 13 조(앱 취약점 점검 대상

) ① 앱 취약점 점검 시기

1. 앱 정보시스템의 취약점 점검은 매년 1 회 이상 진행하는 것을 원칙으로 한다.

② 취약점 점검 대상

1. 모바일 기기
2. 앱 서비스

제 14 조(앱 취약점검방법의 결정)

① 앱 반복 설치 시 오류 발생시 앱 삭제 시 삭제되지 않고 남아있는 파일 및 디렉토리가 없도록 확실히 삭제되도록 수정한다.

② 앱 설치 전후 비정상적인 파일 및 디렉토리 설치 시 설치되는 패키지 내부나 그 외 저장소에 의심되는 파일이나 디렉토리가 존재할 경우 해당 파일 및 디렉토리의 용도를 확인한 후 불필요할 경우 즉시 삭제하고 바이러스 검사 등을 수행한다.

③ 불필요하거나 과도한 권한 설정 시 앱에 실제 사용하는 기능 및 권한이 AndroidManifest.xml8) 파일에서 선언된 권한 간 차이점이 발견될 경우 해당 권한에 대한 요구사항을 분석하고, 불필요하거나 과도한 권한은 수정하거나 삭제한다.

④ 임의기능 등 악성행위 기능 존재 시 앱 설치 및 실행 후 알 수 없는 포트가 LISTEN 상태로 열려있는 경우 해당 포트의 통신이 악의적인지를 검토하고 포트 백도어(backdoor) 여부를 확인 후 보안취약점이 확인되면 해당 기능에 대하여 수정한다.

⑤ 정보 외부 유출 전송되는 정보가 허가된 주소 이외의 다른 주소로 전송될 경우 관련 정보(사용되는 라이브러리, 전송되는 정보 등)를 확인하고 외부로 정보가 유출된다고 판별되면 관련 라이브러리나 컴포넌트에 대한 삭제 또는 수정한다.

⑥ 자원고갈(개발자의 코딩 오류로 인한 비정상적인 자원 사용) 배터리 · 트래픽 점검 앱을 이용하여 비정상적으로 많은 배터리 및 트래픽을 발생시키는지를 확인 후 수정한다.

제 15 조(앱 취약점 점검도구의 선정)

① 앱 취약점 정보, 신규 취약점 업데이트 기능, 앱 취약점 점검결과의 정확성, 앱 취약점 점검결과 보고서, 사용자의

편의성, 점검도구의 안정성을 고려하여 점검도구를 선정한다.

제 16 조(앱 취약점 점검 도구)

① adb 는 Android 운영체제 모바일 기기를 PC 에서 다양하게 제어할 수 있도록 해주는 프로그램으로, 기기에서 다양한 명령어를 실행하는 데 사용할 수 있는 Unix 셸에 관한 액세스를 제공하는 웹 취약점 도구 입니다

② Putty 는 가장 널리 사용되는 ssh 접속 프로그램으로, 직관적인 인터페이스로 사용이 간편하고 freeware 라는 장점을 가지고 있다.

③ apktool 는 안드로이드 애플리케이션(Android Application) 대상의 리버스 엔지니어링 도구입니다.

④ BurpSuite(BurpSuite 는 웹 애플리케이션 보안을 테스트하고 분석하기 위한 Java 애플리케이션입니다.

⑤ Fiddler 는 컴퓨터와 웹 서버 또는 서버 사이의 HTTP 및 HTTP 트래픽을 기록, 검사 및 변경하는 데 사용되는 디버깅 프록시 서버 도구입니다.

⑥ WireShark 는 패킷 스니퍼 , 프로그램 사용 및 프로토콜 분석기 캡처 기능을 제공하는 네트워크 패킷 분석 프로그램입니다.

⑦ Xcode 는 애플 iOS 운영체제 기반의 앱을 개발하고 분석할 수 있는 개발도구 입니다

⑧ iTunes 는 Mac 이나 PC 에서는 iTunes 를 이용하여 모바일 기기와 연결하고 애플리케이션 설치 및 삭제 등 동기화 제공 도구입니다.

제 17 조(앱 취약점 점검 도구 관리)

① 앱 취약점 점검도구의 사용 및 관리는 정보보호책임자로 제한한다.

② 정보보호책임자는 앱 취약점 점검도구의 접근통제에 대한 관리책임을 지며, 새로운 취약점이 발견될 경우 취약점 점검도구의 앱 취약점 데이터베이스에 대한 업데이트를 실시한다.

제 18 조(앱 취약점 점검항목의 선정)

① 정보시스템자산에 문제가 발생하거나 또는 발생할 수 있는 위협요인을 식별하여, 점검에 필요한 앱 취약점은 '안전행안부 취약점 항목' 기준으로 점검항목으로 선정한다.

제 19 조(앱 취약점 점검의 수행)

① 침해사고대응팀은 분석.평가 시 발견된 미 준수 항목 및 정보보호 취약점을 평가한 후 취약점 분석.평가 결과를 앱 취약점과 관련된 각 관리부서에 전달한다. 취약점 분석. 평가 결과에는 다음 각 항목의 내용이 포함되어야 한다.

1. 앱 취약점 분석 평가 수행 일시
2. 앱 취약점 분석 평가 대상
3. 앱 취약점 분석 방법
4. 앱 취약점 점검 내용 및 결과
5. 앱 취약점 조치 가이드 라인

제 20 조(발견된 앱 취약점의 조치)

① 앱 취약점 점검을 통해 발견된 취약점에 대해서 적절한 조치와 해결책을 마련하도록 한다.

② 앱 취약점 점검결과에 대해 기존 정보보호대책의 적정성, 효율성 및 문제점을 평가하고 분석한다.

③ 정보보호대책(방침, 절차, 시스템) 등의 보완이 필요할 경우 기존 대책과 연계하여 효과성, 경제성을 바탕으로 가장 효율적인 대책과 추진방법을 선정한다.

④ 앱 취약점 조치가 완료되면 [첨부 2]앱 취약점 사후 조치보고서를 작성후 정보보호책임자에게 제출한다.

제 4 장 클라우드 인프라 취약점 점검

제 21 조(클라우드 취약점 점검 대상)

① 웹 취약점 점검 시기

1. 클라우드 정보시스템의 취약점 점검은 매년 1 회 이상 진행하는 것을 원칙으로 한다.

클라우드 정보시스템의 최초 구축이나 전환사업 수행시 1 회 점검한다

1. 클라우드 서버
2. 클라우드 서비스
3. 클라우드 가상 웹

22 조(클라우드 취약점검방법의 결정)

① root 계정 원격 접속 제한은 root 계정의 원격 접속 차단 설정 여부를 점검하여 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하는지 점검합니다.

② 패스워드 복잡성 설정은 시스템 정책에 사용자 계정(root 및 일반 계정 모두 해당) 패스워드 복잡성 관련 설정이 되어 있는지 점검합니다.

③ 계정 잠금 임계값 설정은 시스템 정책에 사용자 로그인 실패 임계값이 설정되어 있는지 점검합니다. 무작위 대입 공격 등으로 시스템에 로그인 시도에 대한 차단을 위하여 임계값 설정을 하는 것을 권고합니다.

④ root 홈 패스 디렉터리 권한 및 패스 설정은 PATH 환경변수에 "."(현재 디렉토리 지칭)가 변수의 앞이나 중간에 포함되어 있다면 일반적인 명령어(예: ls, mv,ps 등)를 실행했을 때, 원래의 명령이 아닌 현재 디렉토리의 파일이 우선적으로 실행됩니다. 악의적인 사용자에 의해 비정상 파일이 실행될 수 있으로, root 계정의 PATH 환경 변수를 점검합니다.

⑤ 패스워드 파일 보호는 일부 오래된 시스템의 경우 패스워드 정책이 적용되지 않아 /etc/passwd 파일에 평문으로 암호가 저장되는 경우가 있습니다. 사용자 계정의 비밀번호가 암호화되어 저장하는지 점검합니다.

제 23 조(클라우드 취약점 점검도구의 선정)

① 클라우드 취약점 정보, 신규 취약점 업데이트 기능, 클라우드 취약점 점검결과의 정확성, 클라우드 취약점 점검결과 보고서, 사용자의 편의성, 점검도구의 안정성을 고려하여 점검도구를 선정한다. 또한 정보시스템자산에 문제가 발생하거나 또는 발생할 수 있는 위협요인을 식별하여, 점검에 필요한 클라우드 취약점은 '안전 행안부 취약점 항목' 기준으로 점검 항목으로 선정한다.

제 24 조(클라우드 취약점 점검 도구)

① 클라우드서비스제공사에서 제공하는 서버 취약점 점검 서비스를 활용한다.

② 클라우드 취약점 점검 도구가 없을 때에는 취약점 점검자가 직접 점검을 원칙으로 한

다. **제 25 조(클라우드 취약점 점검 도구 관리)**

① 취약점 점검도구의 사용 및 관리는 정보보호책임자로 제한한다.

② 정보보호책임자는 클라우드 취약점 점검도구의 접근통제에 대한 관리책임을 지며, 새로운 취약점이 발견될 경우 취약점 점검도구의 클라우드 취약점에 대한 조치를 실시한다.

제 25 조(발견된 클라우드 취약점의 조치)

① 클라우드 취약점 점검을 통해 발견된 취약점에 대해서 적절한 조치와 해결책을 마련하도록 한다.

② 클라우드 취약점 점검결과에 대해 기존 정보보호대책의 적정성, 효율성 및 문제점을 평가하고 분석한다.

③ 정보보호대책(방침, 절차, 시스템) 등의 보완이 필요할 경우 기존 대책과 연계하여 효과성, 경제성을 바탕으로 가장 효율적인 대책과 추진방법을 선정한다.

④ 클라우드 취약점 조치가 완료되면 [첨부 3]클라우드취약점 사후 조치보고서를 작성후 정보보호책임자에게 제출한다.

제 5 장 부칙

제 27 조(시행일)

본 지침은 정보보호위원회 의결 완료일부터 시행된다.

제 28 조(예외적용)

다음 각 호에 해당하는 경우에는 본 지침에서 명시한 내용일지라도 정보보호 최고 책임자의 승인을 받아 예외 취급할 수 있다.

① 기술환경의 변화로 적용이 불가능할 경우

② 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우

③ 기타 재해 등 불가항력적인 상황일 경우

제 29 조(경과조치)

특별한 사유에 의하여 본 지침에 정하는 요건을 충족하지 못한 경우에는 발생일로부터 3 개월 이내에 개선방안을

강구하여야 한다.

[첨부 1] 웹 취약점 사후 조치보고서

점검사항	점검결과	조치여부	조치확인	비고
크로스 사이트 스크립팅				
삽입 취약점				
악성 파일 실행				
불안전한 직접객체 참조				
크로스 사이트 요청 참조				
정보유출 및 부적절한 오류처리				
취약한 인증 및 세션 관리				
불안전한 암호화 저장				
불안전한 통신				
URL 접근제한 실패				
디렉토리 리스팅				
부적절한 환경 설정				
파일 다운로드				
파일 업로드				
백업파일 노출				
입력값 검증 부재				
쿠키(Cookie) 암호화				
취약한 접근 통제				
서비스 거부 공격				
버퍼 오버플로우				
가짜 액티브(Active) X 확인하기				
티맥스 WAS(JEUS) 취약점				

[첨부 2] 앱 취약점 사후 조치보고서

점검사항	점검결과	조치여부	조치확인	비고
반복 설치 시 오류 발생				
앱 설치 전후 비정상적인 파일 및 디렉토리 설치				
불필요하거나 과도한 권한 설정				
앱 삭제 후 안전성				
기능의 정상동작				
임의기능 등 악성행위 기능 존재				
정보 외부 유출				
자원고갈				
루팅 및 탈옥 기기에서의 정상 동작				
ID 값의 변경				
동일키로 서명된 서로 다른 앱 간의 UID 공유				
인텐트 권한의 올바른 설정				
인증 정보 생성 강도 적절성				
중요정보의 평문 저장 및 전송				
중요정보 저장 및 전송 시 취약한 암호알고리즘 적용				
기타 중요 정보의 평문 저장 및 전송				
기타 중요 정보 저장 및 전송 시 취약한 암호 알고리즘 적용				
파일 다운로드시 외부주소 및 파일 무결성 우회				
개인정보 및 개인위치정보 수집 및 활용에 대한 동의				
난독화				

[첨부 3] 클라우드 취약점 사후 조치보고서

점검사항	점검결과	조치여부	조치확인	비고
root 계정 원격 접속 제한				
패스워드 복잡성 설정				
계정 잠금 임계값 설정				
패스워드 파일 보호				
root 홈 패스 디렉터리 권한 및 패스 설정				
파일 및 디렉터리 소유자 설정				
/etc/passwd 파일 소유자 및 권한 설정				
/etc/shadow 파일 소유자 및 권한 설정				
/etc/hosts 파일 소유자 및 권한 설정				
/etc/(x)inetd.conf 파일 소유자 및 권한 설정				
/etc/syslog.conf 파일 소유자 및 권한 설정				
/etc/services 파일 소유자 및 권한 설정				
SUID,SGID,Stick bit 설정 파일 점검				
사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정				
world writable 파일 점검				
/dev에 존재하지 않는 device 파일 점검				
$HOME/.rhosts, hosts.equiv 사용 금지				
접속 IP 및 포트 제한				
finger 서비스 비활성화				
Anonymous FTP 비활성화				
r 계열 서비스 비활성화				

cron 파일 소유자 및 권한설정				
Dos 공격에 취약한 서비스 비활성화				
NFS 서비스 비활성화				
NFS 접근 통제				
automountd 제거				
RPC 서비스 확인				
NIS , NIS+ 점검				
tftp, talk 서비스 비활성화				
Sendmail 버전 점검				
스팸 메일 릴레이 제한				
일반사용자의 Sendmail 실행 방지				
DNS 보안 버전 패치				
DNS Zone Transfer 설정				
Apache 디렉토리 리스팅 제거				
Apache 웹 프로세스 권한 제한				
Apache 상위 디렉토리 접근 금지				
Apache 불필요한 파일 제거				
Apache 링크 사용 금지				
Apache 파일 업로드 및 다운로드 제한				
Apache 웹 서비스 영역의 분리				
최신 보안패치 및 벤더 권고사항 적용				
로그의 정기적 검토 및 보고				
root 이외의 UID가 '0' 금지				
root 계정 su 제한				

패스워드 최소 길이 설정				
패스워드 최대 사용 기간 설정				
패스워드 최소 사용기간 설정				
불필요한 계정 제거				
관리자 그룹에 최소한의 계정 포함				
계정이 존재하지 않는 GID 금지				
동일한 UID 금지				
사용자 shell 점검				
Session Timeout 설정				
hosts.lpd 파일 소유자 및 권한 설정				
NIS 서비스 비활성화				
UMASK 설정 관리				
홈디렉토리 소유자 및 권한 설정				
홈디렉토리로 지정한 디렉토리의 존재 관리				
숨겨진 파일 및 디렉토리 검색 및 제거				
ssh 원격접속 허용				
ftp 서비스 확인				
ftp 계정 shell 제한				
Ftpusers 파일 소유자 및 권한 설정				
Ftpusers 파일 설정				
at 파일 소유자 및 권한 설정				
SNMP 서비스 구동 점검				
SNMP 서비스 커뮤니티스트링의 복잡성 설정				
로그온 시 경고 메시지 제공				

NFS설정파일접근권한				
expn, vrfy 명령어 제한				
Apache 웹서비스 정보 숨김				
정책에 따른 시스템 로깅 설정				