Confidential

# 인프라 취약점진단 수행계획서

2025. 08. 13.

## Confidentiality Agreements

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격 하게 제한됩니다.

본 보고서는 SK쉴더스에서 작성을 하였으며, 정보보호 서약에 대한 사항을 준수 합니다.

# - 목 차 -


**1. 개요 ..... 4**

1.1. 목적 ..... 4

1.2. 진단방법 ..... 4

1.3. 진단일정 ..... 4

1.4. 진단대상 ..... 5

1.5. 진단절차 ..... 6

1.6. 진단항목 ..... 7

1.7. 진단 평가 기준 ..... 7

**2. 진단결과 ..... 8**

2.1. 수행 산출물 ..... 8

2.2. 수행 후의 조치사항 ..... 8

2.3. 협조 및 유의사항 ..... 8

# 1. 개요

## 1.1. 목적

본 인프라 진단은 **"J.W.P. MagicShop"**에서 운영중인 주요 정보시스템에 대하여 인터넷을 통해 접근하여 악용할 수 있는 취약성이 존재하는지 또는 내부 직원이나 내부망에 거점을 확보한 자가 악용할 수 있는 취약성이 존재하는지를 점검하고, 발견된 취약성에 대한 대응책을 수립하여 안전하고 신뢰할 수 있는 정보시스템 구축 및 운영을 위한 기반을 마련 및 보안수준 향상을 위한 방법을 제시하고자 합니다.

## 1.2. 진단방법

정보시스템 관리/운영 부문과 기술적 부문에 대한 취약성을 진단하고 관리자 인터뷰를 통해 대상 시스템을 점검합니다.

○ 쉴더스 취약점 점검 도구인 SENUS를 사용한 자동진단 및 분석 수행

○ 인프라 장비 담당자 인터뷰 수행을 통한 현황 파악 및 분석 수행

## 1.3. 진단일정

인프라 취약점진단 수행 일정은 사전준비 및 공조체계 마련, 서버 취약점 점검, 점검결과 분석, 보고서 작성의 4단계로 수행하며, 세부 일정은 다음과 같습니다.

| 구분 | 내용 | 일정 |
|---|---|---|
| 사전준비 | 대상협의 및 환경분석 | 2025.08.01 ~ 2025.08.09 |
| 취약점 점검 | 취약점 점검 수행(자동/수동) | 2025.08.11 ~ 2025.09.05 |
| 결과분석 / 보고서 | 결과분석 및 보고서 작성 | 2025.09.05 ~ 2025.09.17 |
| 결과보고서 제출 | 최종 결과보고서 제출 | 2025.09.17 (종료) |

[표 1 – 진단일정]

### 1.4. 진단대상

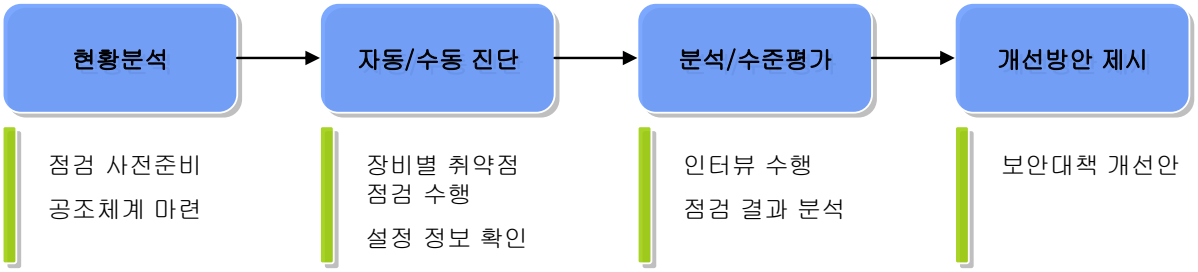
인프라진단 대상의 상세 내역은 다음과 같습니다.

| No | 구분 | 호스트명 | IP Address | 버전 |
|---|---|---|---|---|
| 1 | OS | jwp-web-01 | 10.0.0.14 | Ubuntu 22.04 LTS |
| 2 | OS | jwp-was-01 | 10.0.4.135 | Debian 12 GNU/Linux 12 (bookworm) |
| 3 | OS | jwp-db-01 | 10.0.8.8 | Windows Server 2019 Datacenter |
| 4 | WEB | jwp-web-01 | 10.0.0.14 | Apache 2.4.52 |
| 5 | WAS | jwp-was-01 | 10.0.4.135 | Tomcat 9.0.107 |
| 6 | DBMS | jwp-db-01 | 10.0.8.8 | Oracle 21c XE |

[표 2 – 인프라 진단대상]

### 1.5. 진단절차

인프라 진단 수행 절차는 아래 그림과 같이 "현황분석", "자동/수동 진단", "분석/수준평가", "개선방안 제시"를 수행하여 최종 취약점 분석 보고서를 작성합니다.




[그림 1 – 취약성 진단 수행 절차]

1. 현황 분석

원활한 진단을 수행하기 위하여 실제 진단 전에 입수된 자료와 담당자 인터뷰등을 통해 대상 웹서버에 대한 정보(IP, Hostname, Service, WAS정보, 웹구조, 네트워크 Config 등)를 수집하며 전반적인 보안현황을 파악합니다.

2. 자동/수동 진단

실제 장비의 취약점을 진단하는 단계로 자동화 진단도구를 이용한 서버 점검(쉴더스 자체 점검 도구 사용) 및 네트워크 Config 점검을 수행합니다.

3. 분석/수준 평가

진단 단계에서 식별된 취약점을 분석하여 문제점을 도출하고, 현재 취약점의 보안 수준을 평가하여 각 장비의 취약점이 미칠 수 있는 위험을 분석 평가합니다.

4. 개선방안 제시

분석 평가된 취약점에 따른 개선방안을 도출하여 이에 따른 보안가이드를 제시합니다.

### 1.6. 진단항목

인프라 진단항목은 「J.W.P. MagicShop-인프라진단수행계획서_별첨_인프라진단항목.xlsx」에 별첨 되어 있습니다.

### 1.7. 진단 평가 기준

| 보안 등급 | 상 | 중 | 하 |
|---|---|---|---|
| 보안수준 점수(%) | 70 이상~100 미만 | 55 이상~70 미만 | 0 이상~ 55 미만 |
| 해커공격<br>대응수준 | 고급해커<br>120시간 공격에 대응 | 중급해커<br>120시간 공격에 대응 | 초급해커<br>120시간 공격에 대응 |

[표 3 – 보안 평가등급(TCSEC)]

※ 평가등급 (TCSEC): 미 국방성 (DoD)의 컴퓨터시스템 보안등급 기준인 TCSEC (Trusted Computer System Evaluation Criteria) 의 개념에 기반하며, 기술적 영역에 대한 기업의 보안환경을 분석하여 그 수준을 진단하고 등급을 평가하는 기준. 기술적 보안에 대해 A ~ E 5 단계 등급과 100점 만점의 보안수준 점수로서 평가

# 2. 진단결과

## 2.1. 수행 산출물

인프라 보안진단을 통하여 제공되는 산출물은 다음과 같습니다.

| No | 작업 산출물 | 제출시기 | 비 고 |
|---|---|---|---|
| 1 | 인프라진단 수행계획서 | 진단 수행 전 | 본 문서 |
| 2 | 인프라진단 결과보고서 | 진단 수행 후 | 서버 취약점 분석평가 결과 |
| 3 | 인프라 이행점검 결과보고서 | 조치 이행 후 | 서버 취약점 이행점검 결과 |

[표 4– 수행 산출물]

## 2.2. 수행 후의 조치사항

1) 작업 수행완료 후 특권 획득 표시 및 기타 흔적들의 삭제(예: /upload/infosec.jsp)
2) 대상 시스템의 정상작동 확인

## 2.3. 협조 및 유의사항

서버 취약점진단의 효율 및 정확성을 보장하기 위하여 다음 사항에 대한 지원을 요청합니다.

1) 대상 서버 중 내부망에 위치한 서버 취약점 진단을 위한 점검용 node 및 IP Address 부여
2) 서버 취약점 진단을 위한 대상 서버의 Administrator 또는 root 계정 확보 요청
3) 서버 별 실무담당자 연락처 요청 (ex. 시스템 담당, 응용 담당, 유지보수 담당자 등)
4) 진단 컨설턴트가 사용할 수 있는 Remote 또는 Local Network Segment 환경의 제공
5) 진단 스크립트 업로드를 위한 FTP, 터미널 서비스 오픈 요청