최종연구보고서	KISA-WP-2013-0008

소프트웨어 보안 취약점 평가 체계 연구

Research on Software Vulnerability Scoring Systems

수 탁 기 관 : 한 국 정 보 보 호 학 회

2013. 08

KISA 한국인터넷진흥원
Korea Internet & Security Agency

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “소프트웨어 보안 취약점 평가 체계 연구”의 최종 연구보고서로 제출합니다.

2013년 08월 30일

수탁 기관 : 한국정보보호학회
연구책임자 : 교 수 안 준 선 (한국항공대학교 항공전자 및 정보통신공학부)
참여연구원 : 교 수 창 병 모 (숙명여자대학교 컴퓨터과학부)
교 수 이 은 영 (동덕여자대학교 컴퓨터학과)

요 약 문

1. 제목

소프트웨어 보안 취약점 평가 체계 연구

2. 연구개발의 목적 및 중요성

본 연구의 목적은 국내 환경에 적합한 소프트웨어 보안 취약점의 중요도 평가 방법론을 제시하는 것이다. 본 연구는 신규 보안 취약점 발굴에 대한 포상, 보안 취약점 데이터베이스 구축 등의 다양한 보안 취약점 대응 사업에 필수적인 기본 자료를 제공한다. 본 연구 결과를 활용하여 보안 취약점 대응의 효율과 효과를 높이고, 취약점 발굴 포상 및 취약점 대응 우선순위 선정의 근거를 확보할 수 있을 것으로 판단된다.

3. 연구개발의 내용 및 범위

국내 환경에 적합한 보안 취약점 평가방법을 개발하기 위하여, 국내외 관련 동향 및 연구 결과에 대한 조사를 수행하며, 대표적인 보안 취약점 및 보안 약점 평가 방법인 CWSS와 CVSS에 대한 연구를 기반으로 국내 취약점 발굴 사례에 대한 시범 평가를 수행한다. 이러한 연구를 기반으로 국내 환경에 맞는 보안 취약점 평가방법을 개발하고, 국내 취약점 발굴 사례에 이를 적용한다.

4. 연구결과

보안 취약점 중요도 정량 평가와 보안 취약점 발굴 포상제에 대한 국

내외 관련 사례 연구 결과를 제공하며, 대표적 보안 취약점 및 약점 평가 방법인 CWSS 및 CVSS에 대한 연구 결과 및 이에 기반한 국내 보안 취약점 보고 사례에 대한 시범 평가 결과를 제시한다. 최종적인 연구 결과로서 국내 환경을 고려한 보안 취약점 평가 방법론 및 이를 적용한 국내 취약점 사례 시범 평가 결과를 제공한다.

5. 활용에 대한 건의

국내 신규 취약점 발굴 포상에 대한 근거 자료 도출에 사용될 수 있으며, 아울러 보안 취약점 데이터베이스 구축 시 중요도 점수를 함께 제공함으로써 보안 취약점에 대한 대응, 교육, 연구, 제품 개발 등에 활용할 수 있다.

6. 기대효과

보안 취약점 중요도에 대한 객관적 자료를 제공함으로써 관련 취약점 대응 사업의 추진에 대한 객관적 근거 제시 및 효율적 추진에 도움이 될 것으로 판단된다.

SUMMARY

1. Title

Research on Software Vulnerability Scoring Systems

2. Purpose of the Study

The purpose of this project is to provide a software vulnerability scoring system which is suitable for Korea environment.

3. Contents and Scope

Firstly, we survey related works on software vulnerability scoring. Among the scoring systems, using CWSS and CVSS, we do a pilot scoring test on recent vulnerability exposures. Then, we develop a new vulnerability scoring system which is suitable for Korean environment. Finally, using our new scoring system, we score recent Korean vulnerability exposure cases to show the usability and objectivity of our system.

4. Results of the Study

We provide survey results on weakness scoring systems and software vulnerability bounties. Our main result is a new software vulnerability scoring system which is suitable for Korean environment. Also, we provide pilot software vulnerability scoring results which are

based on CWSS, CVSS and our new scoring method.

5. Possible Applications of the Study

Our scoring system can be used for software vulnerability bounty programs to estimate the usefulness of new software vulnerability exposures. Also, our scoring method can be used to develop a software vulnerability database such as NVD (National Vulnerability Database) of USA.

6. Expected Effects

Using the scoring system, vulnerability bounty programs can acquire objectivity in assessment of new vulnerability exposures. Also, we can prioritize handling of various vulnerabilities and make computer system environments secure more efficiently and effectively.

목 차

제 1 장 서 론 ····· 1

제 1 절 과제의 필요성 ····· 1

제 2 절 과제의 목표 및 내용 ····· 4

제 2 장 국내외 동향 조사 ····· 9

제 1 절 CVSS (Common Vulnerability Scoring System) ····· 9

제 2 절 CWSS (Common Weakness Scoring System) ····· 26

제 3 절 보안 취약점 데이터베이스 ····· 32

제 4 절 국내외 취약점 포상 사례 ····· 41

제 3 장 CVSS 시범평가 ····· 67

제 1 절 CVSS 평가 항목 및 평가 기준 ····· 67

제 2 절 국내 보안 취약점 사례에 대한 시범평가 ····· 79

제 3 절 시범평가 결과 ····· 121

제 4 장 CWSS 시범평가 ····· 131

제 1 절 CWSS 평가 항목 및 평가 기준 ····· 131

제 2 절 국내 보안 취약점 사례에 대한 시범평가 ····· 144

제 3 절 CWSS 시범평가 결과 ····· 204

제 5 장 소프트웨어 대상 신규 취약점 평가방법 연구 ····· 219
제 1 절 서론 ····· 219
제 2 절 기존 보안 취약점 및 보안약점 평가 방법 개요 ····· 220
제 3 절 평가 척도의 설정 ····· 221
제 4 절 중요도 점수의 산정 ····· 241

제 6 장 결론 ····· 244

Table of Contents

Chapter 1. Introduction ····· 1

Section 1. Necessity of the research ····· 1

Section 2. Objectives of the research ····· 4

Chapter 2. Survey on Current Trends ····· 9

Section 1. CVSS (Common Vulnerability Scoring System) ····· 9

Section 2. CWSS (Common Weakness Scoring System) ····· 26

Section 3. Vulnerability Databases ····· 32

Section 4. Vulnerability Reward Programs ····· 41

Chapter 3. CVSS Vulnerability Evaluation ····· 67

Section 1. CVSS Metrics and Measures ····· 67

Section 2. Result of Vulnerability Evaluation ····· 79

Section 3. Analysis of Vulnerability Evaluation ····· 121

Chapter 4. CWSS Vulnerability Evaluation ····· 131

Section 1. CWSS Metrics and Measures ····· 131

Section 2. Result of Vulnerability Evaluation ····· 144

Section 3. Analysis of Vulnerability Evaluation ····· 204

Chapter 5. Development of New Scoring System ····· 219

Section 1. Introduction ····· 219

Section 2. Outline of Existing Vulnerability Scoring Systems ·· 220

Section 3. Metrics of New Scoring System ····· 221

Section 4. Equations of Calculating Scores ····· 241

Section 5. Result of Vulnerability Evaluation ····· 244

Section 6. Analysis of Vulnerability Evaluation ····· 304

Chapter 6. Conclusion ····· 309

그림 목차

(그림 2-1) CVSS 메트릭 그룹 ····· 10
(그림 2-2) CVSS 메트릭과 공식의 관계 ····· 11
(그림 2-3) CVSS v3의 Base 평가척도 ····· 25
(그림 2-4) 환경에 따른 경감 ····· 25
(그림 2-5) CWSS 메트릭 그룹과 그룹별 하위 요소들 ····· 28
(그림 2-6) CVSS 계산기 예시 ····· 32
(그림 2-7) CVE 항목대상 CVSS 측정 예 ····· 33
(그림 2-8) CVSS 기본점수: High / Medium / Low ····· 34
(그림 2-9) CNVD 홈페이지 ····· 36
(그림 2-10) 대중적인 취약점 처리 프로세스 ····· 38
(그림 2-11) CNVD 취약점 처리 프로세스 ····· 38
(그림 2-12) CNVD 홈페이지에서 취약점 제출 화면 ····· 39
(그림 2-13) CNVD 취약점 보고 예시 ····· 40
(그림 2-14) 크롬 프로젝트 ····· 45
(그림 2-15) 어베스트사 버그바운티 ····· 51
(그림 2-16) 제로데이 이니셔티브 프로그램 ····· 59
(그림 2-17) 제로데이 이니셔티브 취약점 보고 예시 ····· 62

표 차례

[표 2-1] 접근 벡터 ····· 12
[표 2-2] 접근 난이도 ····· 13
[표 2-3] 인증 ····· 14
[표 2-4] 기밀성 영향 ····· 15
[표 2-5] 무결성 영향 ····· 15
[표 2-6] 가용성 영향 ····· 16
[표 2-7] 공격 가능성 ····· 17
[표 2-8] 대응 수준 ····· 18
[표 2-9] 보고 신뢰성 ····· 18
[표 2-10] 부수적 피해 잠재성 ····· 19
[표 2-11] 대상 분포 ····· 20
[표 2-12] 보안 요구 ····· 21
[표 2-13] 권한범위 평가척도 ····· 22
[표 2-14] 영향범위 평가척도 ····· 23
[표 2-15] 필요한 권한 평가척도 ····· 23
[표 2-16] 사용자 상호작용 평가척도 ····· 24
[표 2-17] CWSS에 포함된 평가 방식 ····· 27
[표 2-18] Base Finding 메트릭 그룹과 하위 요소 ····· 29
[표 2-19] Attack Surface 메트릭 그룹과 하위 요소 ····· 30
[표 2-20] Environment 메트릭 그룹과 하위 요소 ····· 31
[표 2-21] 구글의 보상프로그램 등급 ····· 45
[표 2-22] ZDI 보상 등급 ····· 60
[표 2-23] 제로데이 이니셔티브 취약점 예 ····· 62

[표 3-1] 국내 보안 취약점 사례 ····· 79
[표 3-2] 평가 항목별 점수 ····· 121
[표 3-3] 평가 메트릭 그룹 요약 ····· 122
[표 3-4] 평가 결과 점수 ····· 126
[표 3-5] 평가 결과 점수: 내림차순정렬 ····· 127
[표 4-1] 국내 보안 취약점 사례 ····· 144
[표 4-2] 평가 항목별 점수 ····· 204
[표 4-3] 보안 취약점 평가결과 (점수순) ····· 206
[표 4-4] 평가 영역별 부분 점수 ····· 209
[표 4-5] “기술적인 영향” 평가 결과 ····· 211
[표 4-6] “공격유형” 평가 결과 ····· 213
[표 4-7] “환경적인 영향” 평가 결과 ····· 216
[표 5-1] 평가 요소별 척도 ····· 223
[표 5-2] 취약점 평가를 위한 평가 척도의 설정 ····· 227
[표 5-3] 목적에 따른 평가 요소의 반영 ····· 242
[표 5-4] 신규 중요도 평가체계 시범평가 결과 ····· 305
[표 6-1] 추진일정 대비 진척도 ····· 310

제 1 장 서 론

제 1 절 과제의 필요성

1. 국내외 소프트웨어 보안 취약점 동향

소프트웨어 소스코드의 보안 약점(weakness)으로 인한 보안 취약점(vulnerability)이 정보 시스템의 보안 침해 예방에 있어 중요한 과제로 제시되고 있으며, 정보 시스템에서 발견되는 이러한 보안 취약점에 대한 효과적이면서도 신속한 대응에 대한 관심이 증가하고 있다. 또한 개발 중인 소프트웨어에 대해서도, 소스코드 내에 존재하는 보안약점들에 대하여 향후 시스템의 보안 취약점을 유발하는 치명적인 약점들을 선별하고 제거하여야 하며, 이러한 작업을 효과적으로 수행하기 위한 다양한 기술적 및 정책적 노력들이 이루어지고 있다.

소프트웨어에서 발생할 수 있는 보안약점과 이를 통해서 발생할 수 있는 보안 취약점에 대한 정보를 축적하고 이를 효과적으로 제공하고자 하는 연구가 활발히 진행되어 지금까지 상당한 진척과 성과를 보이고 있으며, 대표적인 사례로는 미국 MITRE 재단의 CVE (Common Vulnerability Enumeration), CWE (Common Weakness Enumeration) 프로젝트와 중요 보안약점을 선별하여 발표하는 CWE/SANS Top 25, OWASP Top 10 등을 들 수 있다. 국내에서는 2009년부터 정보시스템 보안강화체계를 시작으로, 소스코드 보안 취약점 진단도구 등과 함께 이에 대한 각종 관리 점검 기준 및 가이드라인 등이 개발되어, SW 소스코드의 보안성 강화를 위한 국가적 측면의 공공 보안 강화 체계를 구축하고 있으며, 공공기관의 정보시스템 구축 시 소프트웨어 개발보안의 수행 의무를 단계적으로 강화하고 있다.

2. 소프트웨어 보안 취약점 평가 체계 동향

현재 가장 대표적인 보안약점 및 보안 취약점 평가 체계로는 CWSS (Common Weakness Scoring System)와 CVSS (Common Vulnerability Scoring System)가 있다.

CWSS는 보안약점의 중요도를 평가하는 체계로서 총체적인 SW 보안약점 명세데이터를 구축하는 CWE 프로젝트의 일환으로 추진되었다. CWE와 CWSS의 특징은 안전한 소프트웨어의 개발과 보안 유지에 책임이 있는 당사자들인 정부, 학계, 산업체들이 모여서 만드는 커뮤니티 형태의 협업이라는 점에 있다. 현재 이 프로젝트는 미국 NCSD (National Cyber Security Division)과 미국 DHS (Department of Homeland Security)의 지원을 받아서 진행되고 있다. CWSS는 소프트웨어에 일반적으로 발생하는 다양한 약점에 대하여 제거의 우선순위를 줄 수 있는 정량적인 기준을 제시한다. 정량적인 기준을 제시하기 위한 다양한 메트릭을 약점 자체의 심각성(Base Finding Metric Group), 공격 측면의 심각성(Attack Surface Matric Group), 환경적 측면의 심각성(Environment Matric Group)으로 분류하여 그 정량적 기준과 함께 제시하고 있으며, 아울러 소프트웨어가 사용되는 도메인에 적응하여 중요성 조정할 수 있는 방법론인 CWRAF (Common Weakness Risk Analysis Framework)를 제시하고 있다. 현재 CWSS는 버전 0.8이 2011년 6월에 발표되었으며, 아직 정식 버전은 발표되지는 않은 상태이다. CWSS의 결과는 2011 SANS Top 25의 선정에 일부 평가 척도가 활용되었다.

CVSS는 보안약점으로부터 실제 발생한 보안 취약점의 중요성을 평가하는 연구결과로 보안 취약점 평가를 위한 일반적인 프레임워크를 제공한다. CVSS는 실제 사용되고 있는 소프트웨어에서 공격에 침해될 수 있는 실제적인 보안 취약점을 대상으로 하기 때문에 CWSS와 차별성을 갖는다. CVSS는 보안 취약점을 본질적인 기본 척도(Base Metric), 시간에 따른 척도 (Temporal Metric), 환경적인 척도 (Environmental Metric)에

따라 평가하도록 하여 보안 취약점의 심각성을 다양한 관점에서 평가하기 위한 방법을 제공하고 있다. 그러나 실제 NVD 등의 제공사례에서는 기본 척도만을 사용하고 있다. 현제 CVSS는 어느 정도 정착 단계에 이르러 버전 2가 주로 활용되고 있으며 다음 버전의 개발에 대한 연구가 진행되고 있다.

3. 국내 환경에 적합한 보안 취약점 평가 체계의 필요성

반면 소프트웨어 보안 취약점은 그 자체의 본질적인 특성 뿐 아니라 사용되는 환경이나 응용 분야의 특성, 소프트웨어 점유율, 시간 및 지역에 따라 변화하는 정보 시스템 환경 등에 영향을 받게 되므로, 국내에서도 이러한 국내 소프트웨어 환경 특성을 고려한 새로운 소프트웨어 보안 취약점 평가 체계를 구축할 필요가 있다. 또한 같은 척도라 할지라도 국내 상황에 맞는 적절한 객관적 기준이 새로 설정되어야 할 것이다. 따라서 국내 환경을 고려한 타당한 정량적 및 정성적 기준을 제시하고 이에 기반 하여 중요 소프트웨어 보안 취약점을 독자적으로 추출할 수 있는 소프트웨어 보안 취약점 평가 체계를 새롭게 구축하는 작업은 국내 소프트웨어 보안성 강화의 지속적인 추진을 위해 반드시 선행되어야 한다.

이러한 소프트웨어 보안 취약점 평가 체계를 새롭게 구축하기 위해서는 먼저 국·내외 보안 취약점 평가 체계 및 적용 관련 활동을 체계적으로 조사할 필요가 있다. 이를 통해서 CVSS, CWSS 등의 장단점을 분석 조사하여야 한다. 또한 NVD (National Vulnerability Database) 및 OSVDB (Open Source Vulnerability Database) 등 보안 취약점 DB의 보안 취약점 평가 체계 적용 방법, 보안 취약점 관련 국제 표준화 추진 동향, 주요 민간업체의 보안 취약점 평가 방법, 국·내외 보안 취약점 포상(Security Bug Bounty) 사례를 통한 보안 취약점 평가 방법 및 적용 사례 등을 조사할 필요가 있다.

보안약점에 대한 정량 평가 방법으로 CVSS, CWSS 등이 제안되어 있

지만, 현재 NVD 등의 데이터베이스 구축에서 사용된 CVSS의 적용 사례는 기본 척도만 사용하고 있어, 보안 취약점의 파급도나 대상 소프트웨어의 점유율 등은 충분히 반영하고 있지 않으며, 나머지 환경적, 시간적 척도도 국내 환경을 적절히 반영하는데 적합한지 확실하지 않으며 기준도 재설정되어야 한다. 또한 CWSS 연구 결과는 약점에 대한 척도라는 점에서 보안 취약점과 어느 정도 차이가 있다는 제약점을 가지며, SANS Top 25 등의 적용 사례에서는 이 중 중요도(importance), 유행도(prevalence), 침해가능성(likelihood of exploit)만 적용하고 있어, 소프트웨어 사용 환경을 반영한 심각성 평가를 적절히 수행하지 못하고 있다.

따라서 국내 소프트웨어의 보안취약점에 적절히 대응하기 위해서는, 기존의 연구 결과를 기반으로 국내 소프트웨어 이용 환경을 고려한 보안 취약점의 파급도, 위험도, 소프트웨어 점유율, 시스템에서의 사용 정도 등을 복합적으로 반영하여 보안 취약점에 대한 심각성을 적절히 평가할 수 있는 기준 및 이를 기반으로 한 평가 방법 개발이 필요하다. 또한 이렇게 개발된 소프트웨어 보안 취약점 평가 체계를 시범적으로 적용하고 그 효용성을 CVSS 및 CWSS 등과 비교하여 개선하는 연구가 병행되어야 할 것이다. 이러한 보안 취약점에 대한 평가체계 연구는 보안 취약점에 대한 다양한 대응 사업을 효율적으로 수행하기 위한 필수적인 기반 데이터로 활용될 수 있을 것으로 판단된다.

제 2 절 과제의 목표 및 내용

1. 과제의 목표

본 과제의 목표는 국내 환경에 적합한 보안 취약점 평가 방법을 연구하고 이를 바탕으로 새로운 보안 취약점 평가 방법을 연구하고 이를 국내 보안 취약점에 시범 적용하는 것이다. 각각에 대해서 요약 정리하면

다음과 같다.

o 국내 환경에 적합한 보안 취약점(Vulnerability) 평가 방법 연구
  - 국내외 보안 취약점 평가 체계와 및 적용 관련 동향 조사 분석
  - 소프트웨어 보안 취약점의 중요도를 정량 평가함에 있어 고려되어야 할 국내 소프트웨어 환경의 특징 연구
  - 소프트웨어 보안 취약점 평가에 국내 환경을 고려한 파급도 및 위험도를 반영하기 위한 방법 연구
  - 국내 환경에 적합한 소프트웨어 보안 취약점 평가 체계 및 객관적 평가 척도 정립 연구

o 소프트웨어 대상 신규 보안 취약점 평가 방법 연구 및 시범 적용
  - 기존 방법에 의한 정량평가를 위한 객관적 기준 설정
  - 기존 보안약점 및 보안 취약점 정량 평가 방법론(CVSS, CWSS) 적용
  - 국내 소프트웨어 환경에 적합한 한국형 보안 취약점 정량 평가 방법 적용
  - 시범 평가 결과 분석 및 추가 개선 수행

2. 주요 연구 내용

본 과제의 목표를 이우기 위한 주요 연구 내용은 크게 다음과 같이 세 가지로 정리할 수 있으며 각각에 대한 설명은 다음 표와 같다.

o 국·내외 보안 취약점 평가 체계 및 적용 관련 동향 조사
o 소프트웨어 대상 신규 보안 취약점 평가 방법 연구
o 보안 취약점 평가 체계 시범 적용

국·내외 보안 취약점 평가 체계 및 적용 관련 동향 조사	
주요 내용	- FIRST의 CVSS (Common Vulnerability Scoring System) 분석 • 한국형 보안 취약점 데이터베이스 구축, 보안 취약점 보상 체계를 위한 기반 연구로서 보안 취약점 중요도 분석 기준에 대한 관련 내용 조사 및 분석 - MITRE의 CWSS (Common Weakness Scoring System) 분석 및 적용사례 조사 • CWSS 평가 척도 및 중요도 계산 방법론 조사 및 분석 - NVD (National Vulnerability Database) 및 OSVDB (Open Source Vulnerability Database) 등 보안 취약점 DB의 보안 취약점 평가 체계 적용 방법 조사 • NVD 및 OSVDB의 전반적인 체계 조사 • NVD와 OSVDB에서는 모두 CVSS의 기본 점수(Base Score)에 가반한 보안 취약점 정량 평가 결과를 제시하고 있으므로 이를 확장하여 실제적인 심각성을 반영하기 위한 방법 연구 - 보안 취약점 관련 국제 표준화 추진 동향 조사 • 보안 취약점에 대한 일관성 있는 정보 제공을 위한 연구 동향과 관련 산학연 활용 동향을 조사함. - Microsoft社, Secunia 등 주요 민간업체의 보안 취약점 평가 방법 및 적용 사례 조사 - 국·내외 보안 취약점 포상(Security Bug Bounty) 사례를 통한 보안 취약점 평가 방법 및 적용 사례 조사 • 취약점 포상을 위한 보안 취약점의 중요도 반영 방법 및 적용 사례 조사 • 본 연구의 보안 취약점 중요도 평가방법 개발에 있어, 포상을 위한 보안 취약점 중요도 평가에 사용되는 주요 척도의 반영 가능성 연구

소프트웨어 대상 신규 보안 취약점 평가 방법 연구	
주요 내용	- 국내 소프트웨어 이용환경을 고려한 보안 취약점의 파급도 및 위험도 평가 연구 • 취약점의 파급도 및 위험도 평가를 위한 객관적 기준 정립 연구 - 소프트웨어 대상 신규 보안 취약점 평가 방법 개발 • 해외 연구 결과와 국내 실정 반영 방법을 적용하여 평가방법 개발
보안 취약점 평가 체계 시범 적용	
주요 내용	- 국내 소프트웨어 보안 취약점 대상 CVSS 및 CWSS 평가 시범 적용 • 국내 보안 취약점 발생 사례에 대한 시범 적용 실시 - 연구 결과로 개발한 보안 취약점 평가 방법 시범 적용 • 국내 보안 취약점 발생 사례에 대한 시범 적용 실시

제 2 장 국내외 동향 조사

제 1 절 CVSS (Common Vulnerability Scoring System)

1. CVSS 소개

이질적이고 다양한 하드웨어와 소프트웨어에 결합되어 있는 취약점을 평가하는 것은 IT 관리 측면에서 매우 중요한 일이다. 평가된 취약점은 우선순위가 부여되어 관리되어야 하며 위험 수준이 높은 순위에 따라 적절한 대처가 취해져야 한다. 그러나 만일 서로 다른 방식으로 측정되고 점수가 부여된 대상들이 모두 긴급한 대처를 요구한다면 IT 관리자는 판단은 어려울 수밖에 없다.

CVSS는 이러한 문제에 대처하기 위한 시도이며 IT 취약점에 대한 영향과 특성을 표현하기 위한 공통 프레임워크를 제공하려는 노력의 결과이다. CVSS는 NIST와 카네기멜론 대학의 연구를 바탕으로 개발되어 현재 FIRST (Forum of Incident Response and Security Teams)에 의하여 관리되고 있는 취약점 평가 표준이다. 공식적인 최신 버전은 2005년에 발표된 2.0 표준이며, 버전 3.0이 내년 발표를 예정으로 검토 중인 것으로 알려져 있다. CVSS는 다음과 같은 이점이 있다.

- o 표준화된 취약성 점수 배점: 만일 조직 내에서 모든 소프트웨어와 하드웨어 플랫폼에 대해 정규화된 취약성 점수 배점을 수행한다면 단일화된 취약점 관리 정책을 강력히 수행할 수 있다. 이런 방식의 정책은 특정 취약점에 대해 얼마나 신속히 검증하고 치료할 수 있는지를 설명하는 서비스 수준 협약 (Service Level Agreement, SLA)과 유사한 것이다.

o 개방형 프레임워크: 만일 취약점이 임의로 배점된다면 사용자들은 이에 대해 혼란을 느낄 수 있다. 어떤 특성 때문에 그러한 점수가 부여되었는지, 지난 번 릴리즈된 것과 지금 것과는 어떻게 다른지 등에 관한 질문이 가능할 것이다. CVSS를 통해 모든 사람들은 점수에 관련된 개별 특성들을 접근할 수 있다.

o 위험 우선순위화: 환경 요소가 점수화된다면 취약점은 상확적인 요소가 된다. 즉 이러한 점수는 어떤 조직의 특정한 위험을 대표하는 점수가 된다는 뜻이다. 사용자는 특정 취약점이 다른 취약점에 비해 어느 정도 중요한지를 인식할 수 있다.

CVSS의 평가항목은 기본(base), 시간(temporal), 환경(environmental)과 같은 세 가지 메트릭 그룹으로 구성된다.

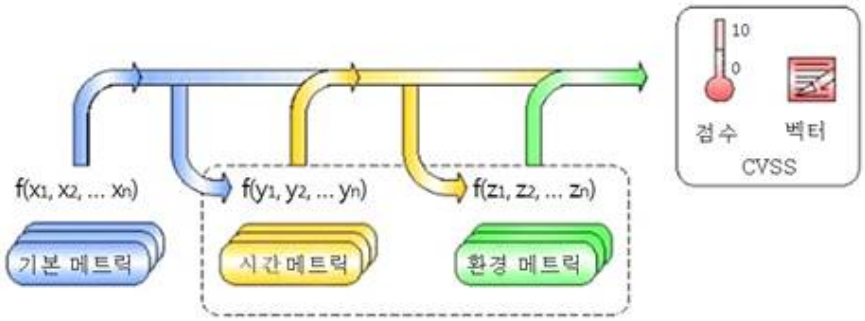
(그림 2-1) CVSS 메트릭 그룹

o 기본 메트릭 그룹: 취약점 특성 중 특정 시간의 흐름이나 사용자 환경에 영향을 받지 않는 특징이며 고유하고 근본적인 특징을 표현하는 평가항목들로 이루어진다.

o 시간 메트릭 그룹: 취약점 특징 중 시간의 흐름에 따라 변할 수 있으나 사용자 환경에는 독립적인 특징을 표현하는 평가항목들로 이루어진다.

o 환경 메트릭 그룹: 취약점 특징 중 특정 사용자 환경에 관련이 있으며 사용자 환경의 특징을 표현하는 평가항목들로 이루어진다.

CVSS 평가에서 중요한 개념 중 하나는 각 메트릭 그룹의 평가항목의 값으로 구성된 벡터이다. 예를 들어 기본 메트릭 그룹 내의 평가항목들의 값으로 구성된 기본 메트릭 벡터가 있으며, 비슷하게 시간 메트릭 벡터, 환경 메트릭 벡터가 있다. CVSS 평가 점수의 핵심은 기본 메트릭 점수(이하 기본 점수라고 함)이며 이 점수는 기본 메트릭 그룹에 속한 평가항목의 값들을 이용하는 계산 공식으로 계산되며 0부터 10 사이의 값을 갖는다. 이 기본 메트릭 점수는 그림 2-2와 같이 시간 메트릭과 환경 메트릭의 점수를 계산하는데 이용된다.



(그림 2-2) CVSS 메트릭과 공식의 관계

(그림 2-2)에서처럼 기본 메트릭 점수은 필요할 경우에 선택적으로 시간 메트릭 점수와 환경 메트릭 점수로 정제될 수 있다. 사용자는 이러한 과정을 통해 사용자 환경에 내제된 취약점 특성을 정교하게 계산에 반영함으로써 유용한 정보로 활용될 수 있다. 각 메트릭 그룹에 대해서 하나씩 살펴보도록 한다.

2. CVSS 메트릭 그룹 및 세부 평가지표

가. 기본 메트릭 그룹

기본 메트릭 그룹은 특정 시간의 흐름이나 사용자 환경에 영향을 받지

않는 취약점에 대한 고유하고 근본적인 특징을 표현한다. 이 그룹은 취약점에 대한 고유 품질을 표현하는 그룹으로서 접근 벡터, 접근 복잡도, 인증, 보안성 영향, 무결성 영향, 가용성 영향 등의 평가항목을 갖는다.

(1) 접근 벡터 (Access Vector, AV)

이 평가항목은 취약점이 어떻게 공격에 이용되는지를 반영한다. 가능한 값의 종류가 [표 2-1]에 나타나 있다. 더욱 원거리의 공격자가 호스트를 공격할 수 있을수록 취약성 점수가 커진다.

[표 2-1] 접근 벡터

평가 값	설명
Local(L)	오직 지역적인 접근을 가지고서 악용할 수 있는 취약점은 공격자에게 취약한 시스템에 대한 물리적 접근이나 지역적인 계정을 가지도록 요구한다. 그 예로 Firewire/USB DMA공격, 지역적 권한 상승(예. sudo)과 같은 외적인 공격을 들 수 있다.
Adjacent Network(A)	인접한 네트워크의 접근을 가지고서 악용할 수 있는 취약점은 공격자에게 브로드캐스트나 취약한 소프트웨어의 충돌 도메인에 대한 접근을 가지도록 요구한다. 지역 네트워크는 지역 IP서브넷, bluetooth, IEEE802.11 그리고 지역 Ethernet 세그먼트를 포함한다.
Network(N)	네트워크의 접근을 가지고서 악용할 수 있는 취약점은 취약한 소프트웨어가 네트워크 스택에 묶여 있고, 공격자에게 지역 네트워크나 지역적인 접근을 요구하지 않는 다는 것을 의미한다. 이런 취약점은 종종 원격에서 악용 가능한 것으로 불린다. 네트워크 공격의 예로는 RPC 버퍼 오버플로우가 있다.

(2) 접근 난이도(Access Complexity, AC)

이 평가항목은 공격자가 이미 목표 시스템에 접근성을 확보한 뒤 취약

점을 얼마나 복잡하게 공격하는지에 관한 측정을 한다. 예를 들면, 인터넷 서비스의 버퍼 오버플로우의 경우 일단 목표 시스템에 들어온 이후 공격자는 자신이 원하는 방향으로 공격을 수행한다.

다른 취약점의 경우 공격을 수행하기 위해 추가적인 활동이 필요하다. 에를 들어 이메일 클라이언트에 대한 취약점의 경우 사용자가 첨부 문서를 다운로드 받고 열어볼 때에만 공격이 가능하다. 가능한 값의 종류가 [표 2-2]에 있으며 접근난이도가 낮을수록 취약성 점수는 높다.

[표 2-2] 접근 난이도

평가 값	설명
High (H)	특화된 접근 조건이 존재한다. 예를 들어 • 대부분의 환경에서 공격자는 미리 상승된 권리나 공격 시스템 외에 부가적인 속임수 시스템을 가져야 한다.(예. DNS hijacking) • 공격은 지식이 있는 사람들에 의해 쉽게 발견될 수 있는 사회 공학 메소드에 의존한다. 예를 들어 피해자는 여러 의심이 가거나 불규칙적인 행동을 수행해야 한다. • 취약한 환경은 매우 드물게 실제 문제로써 보인다. • 만약 경쟁상태가 존재한다면 윈도우는 매우 제한된다.
Medium (M)	접근 조건은 다소 특화되어 있다. 예를 들어 • 공격자는 몇몇의 다소 신뢰할 수 없는 권리 레벨에서의 시스템이나 사용자 그룹에 제한된다. • 몇몇의 정보는 성공적인 공격이 나오기 전에 수집되어야 한다. • 영향을 받은 환경은 디폴트가 아니며, 일반적으로 구성되어 있지 않다 (예. 취약점은 서버가 특정 스키마를 통해 사용자 계정 인증을 수행할 때 나타나지만 또 다른 인증 스키마에서는 나타나지 않는다.) • 공격자는 경우에 따라 신중한 사용자를 속일지 모르는 사회 공학의 작은 부분을 요구한다.(예: 웹 브라우저의 상태 바를 다른 링크로 보이게 변경하는 피싱 공격)
Low (L)	특화된 접근 조건이나 참작할 만한 환경은 존재하지 않는다. 예를 들

	어 • 영향을 받은 제품은 전형적으로 시스템과 사용자의 넓은 범위에 대한 접근을 요구한다. • 영향을 받은 환경은 디폴트며 어디에나 있을 수 있다. • 공격자는 수동적으로 수행될 수 있으며, 사소한 기법이나 부가적인 정보 수집 요구한다. • 경쟁 상황은 느슨한 것들 중 하나이다.

(3) 인증 (Authentication, Au)

이 평가항목은 공격자가 목표 시스템에 침투하기 위해서 몇 번의 인증을 받아야 하는지를 측정한다. 이 평가항목은 인증 프로세스의 복잡도나 강도를 재는 것은 아니며 단지 공격자가 침투하기 위해 필요한 인증 횟수를 잰다. 이 평가항목의 가능한 값들은 [표 2-3]에 나타나 있다. 적은 수의 인증 횟수가 요구될수록 취약성 점수는 높다.

[표 2-3] 인증

평가 값	설명
Multiple (M)	취약점 악용하기 위해서 공격자는 두 번이상의 인증을 해야하며, 심지어 각 시도에 몇몇의 인증서가 사용된다. 어플리케이션에 대한 접근 증명서를 제공하는 것 외에 OS에 대한 공격자 인증이 일어난다.
Single (S)	취약점에 접근하여 악용하는데 단 한 번의 인증을 요구한다.
None (N)	인증이 요구되지 않는다.

(4) 기밀성 영향 (Confidentiality Impact, C)

이 평가항목은 성공적으로 공격된 취약점에 대한 기밀성 영향을 측정한다. 기밀성은 인가된 사용자에게만 접근을 제한하거나 감추어지도록

정보를 관리하며 동시에 인가되지 않은 사용자에게는 접근을 사전에 차단하거나 은폐시키는 것을 말한다. 이 평가항목의 가능한 값들은 [표 2-4]에 나타나 있다. 기밀성 영향이 증가할수록 취약성 점수는 높다.

[표 2-4] 기밀성 영향

평가 값	설명
None(N)	시스템의 기밀성에 영향을 미치지 않는다.
Partial(P)	상당한 정보의 누출이 있다. 몇몇의 시스템 파일에 대한 접근이 가능하다. 그러나 공격자는 획득한 것을 넘어 제어할 수 없으며, 손실의 범위를 제한한다. 예로서 DB에서 오직 일정한 테이블만이 노출 되는 취약점이 있을 수 있다.
Complete (C)	모든 시스템 파일을 드러내는 결과를 낳게 되는 완전한 정보의 누출이 있다. 공격자는 시스템의 모든 데이터를 읽을 수 있다.(메모리, 파일 등등)

(5) 무결성 영향 (Integrity Impact, I)

이 평가항목은 취약점이 성공적으로 공격되었을 때의 영향을 측정한다. 무결성이라 정보에 대한 신뢰도 (trustworthiness)와 보증된 정확도를 나타낸다. 이 평가항목의 가능한 값들은 [표 2-5]에 나타나 있다. 무결성 영향이 클수록 취약성 점수는 높다.

[표 2-5] 무결성 영향

평가 값	설명
None(N)	시스템 무결성에 대한 영향은 없다.

Partial(P)	몇몇 시스템 파일이나 정보의 변경이 가능하다. 그러나 공격자는 변경될 수 있는 것을 넘어선 제어를 할 수는 없으며, 공격자가 영향을 미칠 수 있는 것의 범주는 제한 되어있다. 예를 들어 시스템이나 어플리케이션 파일은 덮여 쓰여 지거나 변경될지 모르지만 역시 공격자는 영향을 받은 파일 이외에는 제어를 할 수 없고 오직 제한된 범주 안에서 변경이 가능하다.
Complete (C)	시스템 무결성이 전체적으로 위험에 드러나 있다. 시스템 보호의 완전한 손실이 있으며, 이는 전체 시스템의 위험 노출로 이어진다. 공격자는 타겟 시스템이 어떤 파일에도 변경을 가할 수 있다.

(6) 가용성 영향 (Availability Impact, A)

이 평가항목은 성공적으로 공격되었을 때의 가용성 영향을 측정한다. 가용성이란 정보 자원의 접근성(accessibility)을 의미한다. 공격자는 네트워크 대역폭, 프로세스 사이클, 디스크 공간 등 시스템 가용성에 영향을 주는 모든 요소를 의미한다. 이 평가항목의 가능한 값들은 [표 2-6]에 나타나 있으며 가용성 영향이 클수록 취약성 점수가 높다.

[표 2-6] 가용성 영향

평가 값	설명
None(N)	시스템의 가용성에 대한 영향은 없다.
Partial(P)	성능이 줄어들거나 자원 이용하는데 방해가 있다. 예를 들어 인터넷 서비스를 위해 성공적인 연결 수에 제한을 두는 네트워크 기반의 플러드 공격이 있다.
Complete (C)	자원이 영향을 받아 완전히 사용할 수 없게 된다. 공격자는 자원을 완전히 이용 못하도록 할 수 있다.

나. 시간 메트릭 그룹

시간 메트릭 그룹은 시간에 따라 변할 수 있는 취약점의 특성을 평가하기 위한 평가 기준으로 공격 가능성, 대응 수준, 보고의 신뢰성 등의 평가항목이 여기에 속한다.

(1) 공격 가능성 (Exploitability, E)

이 평가항목은 공격을 위한 방법이나 코드의 존재 여부에 따라 공격의 용이성을 평가한다.

[표 2-7] 공격 가능성

평가 값	설명
Unproven(U)	이용할 수 없는 공격 코드이거나 완전히 이론상으로 가능한 것이다.
Proof-of-concept (POC)	공격의 개념을 시험하거나, 실제적으로는 대부분의 시스템에는 맞지 않는 공격 시연이 이용가능하다. 그 코드나 기술은 모든 환경에 작용하지 않고, 숙련된 공격자에 의한 많은 변경을 필요로 할지 모른다.
Functional (F)	기능적 공격코드가 이용가능하다. 그 코드는 취약점이 발견된 대부분의 상황에서 영향을 미칠 수 있다.
High(H)	각 취약점은 기능 모바일 자발적인 코드에 의해 악용가능하며, 또 공격이 요구되지 않고(수동 트리거) 자세한 사항은 넓게 이용가능하다. 코드는 모든 상황에서 영향을 미칠 수 있으며, 실질적으로 모바일 자발적인 에이젼트(웜이나 바이러스 같은)를 경유하여 전파 된다.
Not Defined (ND)	메트릭에서 이 값은 점수에 영향을 미치지 않는다.

(2) 대응 수준 (Remediation Level, RL)

이 평가항목은 취약점에 대한 우선순위 설정을 위한 중요한 요소이다. 일반적으로 취약점이 발표될 시점에는 적절한 패치가 없는 경우가 많으며, 공식적인 패치나 업그레이드의 발표 이전에 비공식적인 회피 방법이나 수정이 발표되기도 한다. 이러한 대응의 단계에 따라 취약점에 대한 평가는 점차적으로 하향 조정될 수 있다.

[표 2-8] 대응 수준

평가 값	설명
Official Fix (OF)	이용 가능한 완전한 벤더 솔루션이 있다. 각 벤더는 발표된 공식 패치를 가지고 있거나 업그레이드가 이용 가능해야 한다.
Temporary Fix (TF)	공식적이긴 하나 임시적인 수정방법이 있다. 이는 벤더가 발표한 임시적인 응급 패치 프로그램, 툴, 임시방편을 포함한다.
Unavailable (U)	이용 가능한 솔루션이 없거나, 그것을 적용하는 것이 불가능하다.
Not Defiled (ND)	메트릭에서 이 값은 점수에 영향을 미치지 않는다.

(3) 보고 신뢰성 (Report Confidence, RC)

이 평가항목은 보안 취약점의 존재와 이로 야기되는 알려진 기술적 문제점에 대한 신뢰도를 평가하기 위하여 사용된다.

[표 2-9] 보고 신뢰성

평가 값	설명
Unconfirmed (UC)	한 개의 확인되지 않은 자원이나 어쩌면 모순 될 수 있는 많은 보고서가 있다. 보고서의 정당성에 대한 기밀이 적으며, 그 예로 해커 언더그라운드로부터 드러난 루머를 들수 있다.
Uncorroborated	어쩌면 독립적인 보안 회사나 리서치 기관을 포함하는 많은 공

(UR)	식적이지 않은 자원이 있다. 그 점에서 모순되는 기술적인 디테일이나 다른 애매모호함이 있을 수 있다.
Confirmed (C)	그 취약점은 벤더나 영향을 받은 기술의 프로그래머에 의해서 알려진다. 그 취약점은 또한 그 존재가 기능성의 발표나 공격 코드의 기술 검증, 일반적인 공격과 같은 외부 이벤트로부터 알려졌을 때 확립되어(confiremed)질 수 있다.
Not Defined (ND)	메트릭에서 이 값은 점수에 영향을 미치지 않는다.

다. 환경 메트릭 그룹

환경 메트릭 그룹은 사용자의 환경의 특성을 반영할 수 있는 평가항목으로 부수적 피해 잠재성, 대상 분포, 보안 요구조건 등의 평가항목이 여기에 속한다.

(1) 부수적 피해 잠재성 (Collateral Damage Potential, CDP)

이 평가항목은 취약점을 이용한 공격이 성공하였을 때 자산이나 장비의 파괴 혹은 도난으로 인해 발생할 수 있는 잠재적인 인적 물적 피해를 측정하며 이로 인해 발생할 수 있는 생산성이나 매출의 경제적 손실도 측정한다.

[표 2-10] 부수적 피해 잠재성

평가 값	설명
None(N)	생명, 물적 자산, 생산성 또는 수익의 잠정적인 손실은 없다.
Low (L)	이 취약점에 대한 성공적인 공격은 약간의 물리적인 손실이나 자산 손실의 결과를 낳는다. 또한 기관의 생산성이나 수익에 손실에도 약간의 영향을 미칠 수 있다.

Low-Medium (LM)	이 취약점에 대한 성공적인 공격은 중간정도의 물리적인 손실이나 자산 손실의 결과를 낳는다. 또한 기관의 생산성이나 수익의 손실에도 어느 정도 영향을 미칠 수 있다.
Medium-High (MH)	이 취약점에 대한 성공적인 공격은 상당한 물리적인 손실이나 자산 손실의 결과를 낳는다. 또한 기관의 생산성이나 수익의 손실에도 상단한 영향을 미칠 수 있다.
High (H)	이 취약점에 대한 성공적인 공격은 비극적인 물리적인 손실이나 자산 손실의 결과를 낳는다. 또한 기관의 생산성이나 수익의 손실에도 비극적인 영향을 미칠 수 있다.
NotDefined (ND)	메트릭에서 이 값은 점수에 영향을 미치지 않는다.

(2) 대상 분포 (Target Distribution, TD)

이 평가항목은 보안 취약점으로 인해 침해가 예상되는 시스템의 범위를 평가하기 위하여 사용된다.

[표 2-11] 대상 분포

평가 값	설명
None(N)	대상 시스템이 존재하지 않거나, 오직 연구실에서만 배치되어 있는 매우 전문화되어있는 것이다. 그 환경의 0%가 위험에 처해 있다.
Low(L)	대상 시스템이 그 환경 안에서만 존재하거나, 작은 규모에서만 존재한다. 그 전체 환경의 1%~25%가 위험에 처해있다.
Medium(M)	대상 시스템이 그 환경 안에서만 존재하거나, 중간정도의 규모에서만 존재한다. 그 전체 환경의 26%~75%가 위험에 처해있다.
High(H)	대상 시스템이 그 환경 안에서만 존재하거나, 상당한 규모에서만 존재한다. 그 전체 환경의 76%~100%가 위험에 처해있다.

평가 값	설명
Not Defined (MD)	이 값은 점수에 영향을 미치지 않는다.

(3) 보안 요구조건 (Security Requirements, CR, IR, AR)

이 평가항목은 취약점 공격으로 영향을 받는 IT 자산의 사용자 환경에서의 기밀성, 무결성, 가용성의 중요도에 따라 CVSS 점수를 조정할 수 있도록 해준다. 즉, 기밀성, 무결성, 가용성의 중요도에 따라 기밀성, 무결성, 가용성 점수에 가중치를 줌으로써 취약성 점수를 조정한다.

[표 2-12] 보안 요구

평가 값	설명
Low(L)	기밀성, 무결성, 가용성의 손실은 기관이나 그 기관에 관계된 개인(예. 직원, 고객)에게 제한적으로 불리한 영향을 끼친다.
Medium (M)	기밀성, 무결성, 가용성의 손실은 기관이나 그 기관에 관계된 개인(예. 직원, 고객)에게 심각하게 불리한 영향을 끼친다.
High(H)	기밀성, 무결성, 가용성의 손실은 기관이나 그 기관에 관계된 개인(예. 직원, 고객)에게 비극적이게 불리한 영향을 끼친다.
Not Defined (MD)	메트릭에서 이 값은 점수에 영향을 미치지 않는다.

3. CVSS 버전 업데이트

현재 CVSS 버전 2는 버전 3 (CVSS v3)로 업데이트가 진행 중이며 2014년6월에 완료될 예정이다. CVSS v3는 지금까지 지적된 CVSS v2의

주요 문제점들을 보완하게 될 것이다. CVSS v2의 주요 문제점과 이를 개선하기 위한 CVSS v3의 안은 다음과 같다.

가. 범위(Scope) 문제

CVSS v2의 기밀성 영향(C), 무결성 영향(I), 가용성 영향(A) 등의 영향의 개념은 호스트 운영체제에 대한 영향으로 그 범위가 제한되어 있다. CVSS v2의 이러한 개념은 최근에 가상화(virtualization), 네트워크 등이 많이 사용되는 컴퓨팅 환경으로 바뀜에 따라 그 문제점이 제기되고 있다. CVSS v3에서는 이러한 문제점을 해결하기 위해 범위(scope)라는 개념을 도입할 예정인데 범위는 크게 권한 범위(Authorization Scope)와 영향 범위(Impact Scope)로 구분된다.

권한 범위(Authorization Scope)는 취약한 컴포넌트에 대한 공격자의 권한의 범위를 평가하기 위한 척도로 그 평가척도 값과 설명은 다음 표와 같다.

[표 2-13] 권한범위 평가척도

평가척도 값	설명
Increased	독립적인 권위로부터의 권한 혹은 취약한 컴포넌트의 모든 자원을 제어할 수 있는 권한.
Component	컴포넌트 자체에 의해서 승인된 권한 혹은 컴포넌트의 사용을 승인하기 위해 사용되는 권한.
Decreased	컴포넌트나 그 하위부분에 의해서 제어된 소스로부터 나온 권한.

영향 범위(Impact Scope)는 취약한 컴포넌트에 대한 공격자의 영향의 범위와 제어의 범위를 평가하기 위한 척도로 응용, 호스트, 가상화, 네트

워크 등에 대한 영향을 측정할 수 있다. 그 평가척도 값과 설명은 다음 표와 같다.

[표 2-14] 영향범위 평가척도

평가척도 값	설명
Increased	취약한 컴포넌트와 무관한 권위에 의해 제어된 정보자원이 주로 영향을 받음.
Component	컴포넌트 자체(혹은 같은 권한)에 의해서 제어된 자원이 주로 영향을 받음.
Decreased	컴포넌트나 그 하위부분에 의해서 제어된 자원이 주로 영향을 받음.

나. 필요한 권한(Privileges Required)

인증(Authentication) 평가척도는 공격자가 목표 시스템에 침투하기 위해서 몇 번의 인증을 받아야 하는지를 측정하기 위한 척도로 도입되었으나 NVD의 조사 결과 90% 이상이 None이었으므로 그 실효성이 거의 없는 것으로 밝혀졌다. 따라서 CVSS v3에서는 인증 평가척도를 제거하고 공격자가 공격하기 위해 필요한 권한을 새로운 척도로 사용할 예정이다.

필요한 권한(Privileges Required) 척도는 공격자가 공격하기 위해 필요한 권한을 나타내는 척도로 None, Low, High, Complete 값으로 평가한다. 각 값에 대한 설명은 다음 표와 같다.

[표 2-15] 필요한 권한 평가척도

평가척도 값	설명
None	권한 없음

Low	낮은 영향이 가능한 권한으로 “Complete” 영향은 줄 수 없는 권한 혹은 덜 심각한 영향이 가능한 권한.
High	상당한 권한으로 1~2개의 “Complete” 영향을 줄 수 있는 권한 혹은 심각한 자원에 대한 “Partial” 영향이 가능한 권한
Complete	3개의 “Complete” 영향을 줄 수 있는 완전한 권한.

다. 사용자 상호작용(User Interaction)

CVSS v3에서는 접근 복잡도(Access Complexity)의 사회 공학 부분을 제거하고 사용자 상호작용(User Interaction)으로 대치할 예정이다. 사용자 상호작용의 평가척도 값과 그 설명은 다음 표와 같다.

[표 2-16] 사용자 상호작용 평가척도

평가척도 값	설명
None	공격 성공을 위해서 사용자와 상호작용이 필요 없음.
Simple	공격 성공을 위해서 사용자의 통상적으로 기대되는 액션(이메일 열기, 링크 클릭, PDF 보기 등)이 필요함.
Complex	공격 성공을 위해서 사용자의 통상적이지 않는 액션이 필요함.

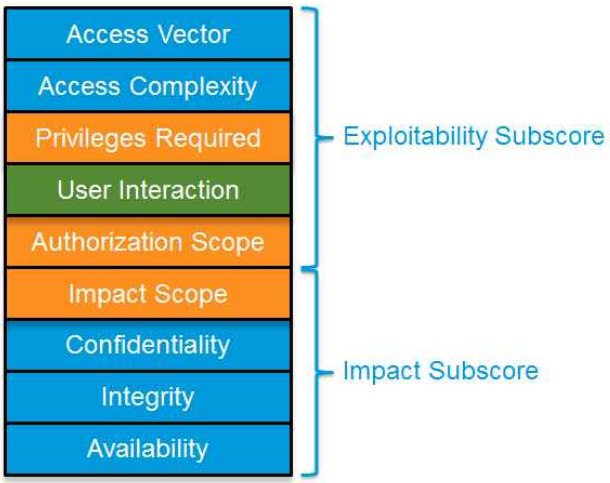
CVSS v3에서는 앞에서 기술한 새로운 평가척도를 포함하여 (그림 2-3)과 같이 공격 가능성 점수 (Exploitability subscore)와 영향 점수(Impact subscore)를 계산할 것이다.

라. 환경에 따른 경감(Mitigated Environmental)

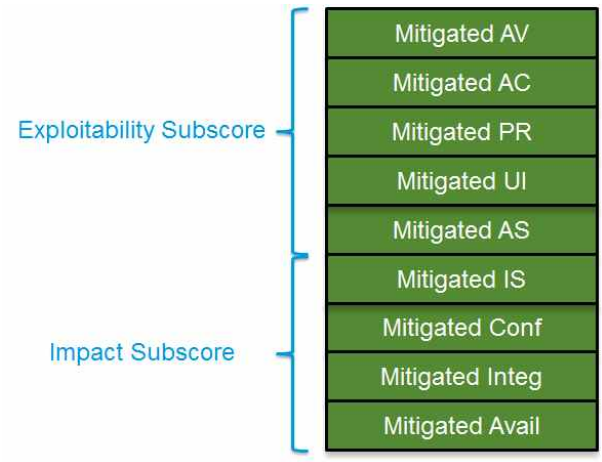
CVSS v3에서 모든 Base 평가척도는 환경에 따라 경감될 수 있다. 환경적인 요소를 고려하여 Base 평가척도를 재계산하도록 한다.

마. 부수적 피해 잠재성, 대상 분포 제거

부수적 피해 잠재성(Collateral Damage Potential), 대상 분포(Target



(그림 2-3) CVSS v3의 Base 평가척도



(그림 2-4) 환경에 따른 경감

Distribution)는 CVSS v1에서 포함된 평가척도로 측정하기 매우 어렵고 큰 조직으로 확대되어 적용되기 어렵다. 따라서 CVSS v3에서는 제거될 예정이다.

제 2 절 CWSS (Common Weakness Scoring System)

1. CWSS 소개

CWSS는 소프트웨어 보안약점의 중요도를 평가하는 평가 체계로 CWE 프로젝트의 일부로 수행되고 있다. CWE와 CWSS의 특징은 안전한 소프트웨어의 개발과 보안 유지에 책임이 있는 당사자들인 정부, 학계, 산업체들이 모여서 만드는 커뮤니티 형태의 협업이라는 점에 있다. 현재 이 프로젝트는 미국 NCSD(National Cyber Security Division)과 미국 DHS (Department of Homeland Security)의 지원을 받아서 진행되고 있다. CWSS는 소프트웨어에 일반적으로 발생하는 다양한 약점에 대하여 제거의 우선순위를 줄 수 있는 정량적인 기준을 제시한다. 정량적인 기준을 제시하기 위한 다양한 메트릭을 약점 자체의 심각성(Base Finding Metric Group), 공격 측면의 심각성(Attack Surface Matric Group), 환경적 측면의 심각성(Environment Matric Group)으로 분류하여 그 정량적 기준과 함께 제시하고 있으며, 아울러 소프트웨어가 사용되는 도메인에 적응하여 중요성 조정할 수 있는 방법론인 CWRAF(Common Weakness Risk Analysis Framework)를 제시하고 있다. 현재 CWSS는 버전 0.8이 2011년 6월에 발표되었으며, 아직 정식 버전은 발표되지는 않은 상태이다.

2. CWSS 메트릭 그룹 (Metric Group)

CWSS의 평가 방식은 대상이 되는 소프트웨어 시스템의 특성과 평가

방식의 특성에 따라서 크게 4가지로 구분된다. [표 2-17]은 4가지 평가 방식의 특성을 설명하고 있다. 현재 CWSS는 targeted 평가 방식과 context-adjusting 평가를 위한 프레임워크를 준비하고 있다. Aggregated 평가 방식에 대한 연구는 향후에 추가될 예정이며, generalized 평가 방

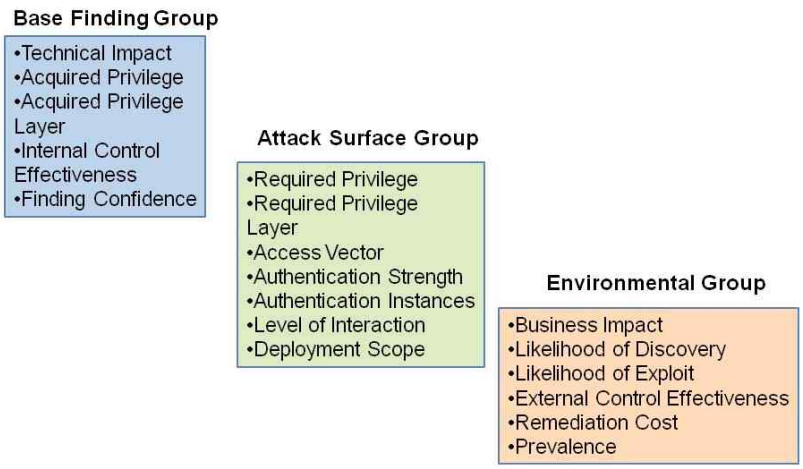
[표 2-17] CWSS에 포함된 평가 방식

방 식	내 용
Targeted (타겟형)	특정한 소프트웨어 패키지의 디자인이나 구현 과정에서 발견되는 개별적인 보안약점에 대해서 평가를 수행하는 방식이다. 예를 들어 특정 FTP 서버 패키지에 포함된 vuln.c라는 소스 파일의 1234 라인에 있는 사용자 인증 코드에서 발견되는 버퍼 넘침 약점에 대한 중요도를 평가하는 방식이다. 자동화된 도구나 소프트웨어 보안 전문가 등이 패키지의 일부로 포함된 소프트웨어의 보안성을 평가하기 위하여 targeted 방식을 사용할 수 있다.
Generalized (일반형)	특정 소프트웨어 패키지에 독립적인 보안약점이나 보안약점 클래스들을 평가하기 위하여 사용되는 방식이다. 이 경우 평가는 각 약점이나 약점 클래스들의 상대적인 우선순위로 표현된다. CWE/SANS Top 25와 OWASP Top 10 등에서 사용되는 방식으로, 일부 자동화된 코드 스캐너에서도 사용된다. Generalized 방식은 특정 패키지 내부에서 모든 취약점의 발생을 모두 분석하는 targeted 방식과는 다른 결과를 낳을 수도 있다. 예를 들어, 버퍼 넘침은 일반적인 경우에서는 위험도가 매우 높은 약점으로 분류되지만, 특정 패키지에서는 ASLR과 같은 OS 수준의 보호 메커니즘에 의해서 공격자에 의해서 직접적으로 이용될 수 없기 때문에 targeted 방식에서는 의외로 중요도가 낮게 평가될 수도 있다.
Context-adjusted (발전형)	서로 다른 분석환경에 따라서 보안약점의 중요도가 조정될 수 있는 방식을 뜻한다. 예를 들어, 사업 모델이나 위협 환경(threat environments), 혹은 위험 허용정도 (risk

방 식	내 용
	tolerance) 등이 고려의 대상이 된다. 이 경우 보안약점이 가지는 일반적인 성격 외에도 상위 레벨의 사업적 고려가 중요도 평가에 영향을 미치게 된다.
Aggregated (통합형)	하위 레벨에서 계산된 다수의 평가 점수를 합산하여 하나의 상위 레벨 점수를 산출하는 방식이다. Aggregated 방식은 targeted 방식과 함께 사용될 수도 있고, 혹은 2010 CWE/SANS Top 25에서 사용되었던 것처럼 generalized 방식과 함께 사용될 수도 있다.

식은 별도로 연구되어 2011년도에 발표된 CWE/SANS Top 25와 CWRAF에 포함되었다.

CWSS에서는 버전 0.6부터 3개의 메트릭 그룹의 18가지 서로 다른 요소 점수를 이용하여 보안약점의 중요도를 계산한다. 3개의 메트릭 그룹은 보안약점의 내재적인 특성과 찾아진 약점의 신뢰도, 그리고 제어의 강도를 표현하는 Base Finding 그룹, 공격자가 존재하는 약점을 찾아내



(그림 2-5) CWSS 메트릭 그룹과 그룹별 하위 요소들

서 이용할 수 있는 난이도를 표현하는 Attack Surface 그룹, 그리고 사업 모델이나 공격 난이도, 외부 제어의 존재 여부를 표현하는 Environmental 그룹으로 나누어진다. (그림 2-5)은 3개의 메트릭 그룹과 그룹별 18개의 하위 요소를 나타낸다.

CWSS는 처음에는 매우 적은 정보를 가지고 중요도 평가를 시작하여, 시간이 지남에 따라 가용 정보의 양과 질이 증가하면서 중요도 평가도 함께 변화하게 된다. 따라서 개별적인 보안약점에 대한 평가 점수는 가용 정보가 변화함에 따라 필연적으로 변화할 수밖에 없다. CWSS 요소 점수는 시간과 환경에 따라 "가변적"이라는 특성을 가지고 있으며, 이 특성은 CWSS가 CVSS와 같은 종류의 요소 점수를 사용할 수 없는 이유가 된다.

가. Base Finding 메트릭 그룹

Base Finding 메트릭 그룹은 보안약점의 내재적인 특성과 찾아진 약점의 신뢰도, 그리고 제어의 강도를 표현하며, [표 2-18]에 표시된 것처럼 5개의 하위 요소를 포함하고 있다.

[표 2-18] Base Finding 메트릭 그룹과 하위 요소

메트릭 그룹	하위요소	평가값
Base Finding	Technical Impact (TI)	C/H/M/L/N/D/Unk /NA/Q
	Acquired Privilege (AP)	A/P/RU/G/N/D /Unk/NA
	Acquired Privilege Layer (AL)	A/S/N/E/D/Unk /NA
	Internal Control Effectiveness	N/L/M/I/B/C/D

	(IC)	/Unk/NA
	Finding Confidence (FC)	T/LT/F/D/Unk/NA/Q

[표 2-19] Attack Surface 메트릭 그룹과 하위 요소

메트릭 그룹	하위요소	평가값
Attack Surface	Required Privilege (RP)	N/G/RU/P/A/D/Unk/NA
	Required Privilege Layer (RL)	S/A/N/E/D/Unk/NA
	Access Vector (AV)	I/R/V/A/L/P/D/U/NA
	Authentication Strength (AS)	S/M/W/N/D/Unk/NA
	Authentication Instances (AI)	N/S/M/D/Unk/NA
	Level of Interaction (IN)	Aut/Ltd/Mod/Opp/High/NI/D/Unk/NA
	Deployment Scope (SC)	All/Mod/Rare/Pot/D/Unk/NA/Q

나. Attack Surface 메트릭 그룹

Attack Surface 메트릭 그룹은 공격자가 존재하는 약점을 찾아내서 이용할 수 있는 난이도를 표현하는 그룹으로, [표 2-19]에 표시된 것처럼 7개의 하위 요소를 포함하고 있다.

다. Environmental 메트릭 그룹

Environmental 메트릭 그룹은 사업 모델이나 공격 난이도, 외부 제어의 존재 여부를 표현하는 그룹으로, [표 2-20]에 표시된 것처럼 6개의 하위 요소를 포함하고 있다.

[표 2-20] Environment 메트릭 그룹과 하위 요소

메트릭 그룹	하위요소	평가값
Environmental	Business Impact (BI)	C/H/M/L/N/D/Unk/NA/Q
	Likelihood of Discovery (DI)	H/M/L/D/Unk/NA/Q
	Likelihood of Exploit (EX)	H/M/L/D/Unk/NA/Q
	External Control Effectiveness (EC)	N/L/M/I/B/C/D/Unk/NA
	Remediation Effort (RE)	E/M/L/D/Unk/NA/Q
	Prevalence (P)	W/H/C/L/D/U/NA/Q

2. CWSS 평가점수 계산법

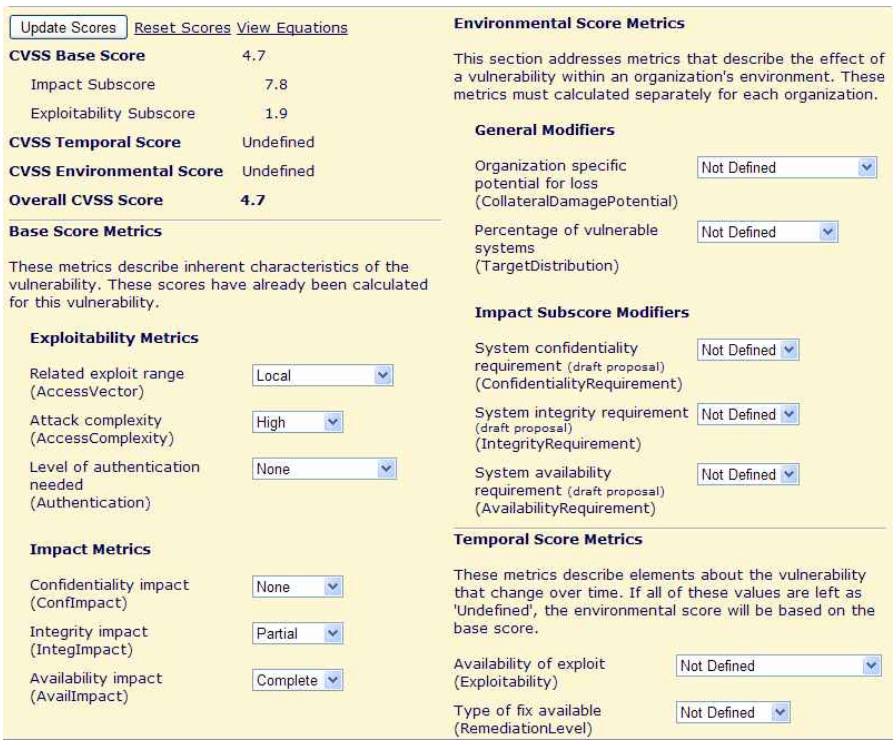
CWSS 버전 0.6의 평가 점수는 0부터 100까지의 숫자로 표현된다. 이 점수는 (Base Finding 점수) * (Attack Surface 점수) * (Environmental 점수) 라는 공식을 이용하여 계산된다. Base Finding 점수는 0부터 100 사이의 점수를 가지며, Attack Surface 점수와 Environmental 점수는 0부터 1 사이의 값을 가지게 된다.

각 부분점수의 평가방식과 의미에 대해서는 4장에서 더 자세히 논의하도록 한다.

제 3 절 보안 취약점 데이터베이스

1. NVD

NVD(National Vulnerability Database)는 보안 콘텐츠 자동화 프로토콜(SCAP)를 사용하여 표현된 미국 정부의 표준 기반 취약점 관리 데이터 저장소이다. 이 데이터는 취약점 관리, 보안 측정 및 규정 준수의 자동화를 가능하게 한다. NVD는 보안 체크리스트, 소프트웨어의 결함, 잘



(그림 2-6) CVSS 계산기 예시

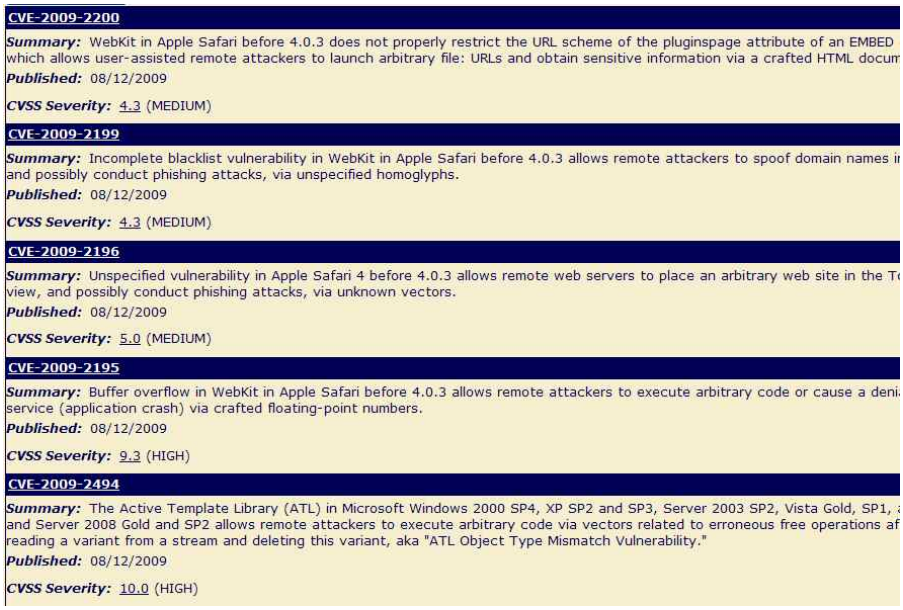
못된 구성, 제품 이름, 평가 메트릭과 관련된 보안 데이터베이스를 포함하고 있다.

(그림 2-6)은 미국의 국가 취약점 데이터베이스(NVD)에서 제공하는 CVSS 메트릭 계산기의 화면이다. (http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:H/Au:N/C:N/I:P/A:C))

다음은 NVD의 취약점 심각도 수준 평가에 관한 기준으로 CVE 항목에 대해 CVSS 벡터 값에 근거하여 산출된 점수에 근거하여 다음과 같은 기준에 의해 심각성 정도(severity)를 정의한다.

o 취약점 심각도 수준 "Low": ····· CVSS 기본 점수 0.0-3.9
o 취약점 심각도 수준 "Medium": ····· CVSS 기본 점수 4.0-6.9
o 취약점 심각도 수준 "High": ····· CVSS 기본 점수 7.0-10.0

NVD는 CVSS 계산 결과에 근거하여 각 취약점에 대해 취약점 심각도 수준을 공개하고 있으며 (그림 2-7)는 NVD에서 제공하는 취약점 항목


CVE-2009-2200
Summary: WebKit in Apple Safari before 4.0.3 does not properly restrict the URL scheme of the pluginspage attribute of an EMBED which allows user-assisted remote attackers to launch arbitrary file: URLs and obtain sensitive information via a crafted HTML docum
Published: 08/12/2009
CVSS Severity: 4.3 (MEDIUM)
CVE-2009-2199
Summary: Incomplete blacklist vulnerability in WebKit in Apple Safari before 4.0.3 allows remote attackers to spoof domain names i and possibly conduct phishing attacks, via unspecified homoglyphs.
Published: 08/12/2009
CVSS Severity: 4.3 (MEDIUM)
CVE-2009-2196
Summary: Unspecified vulnerability in Apple Safari 4 before 4.0.3 allows remote web servers to place an arbitrary web site in the T view, and possibly conduct phishing attacks, via unknown vectors.
Published: 08/12/2009
CVSS Severity: 5.0 (MEDIUM)
CVE-2009-2195
Summary: Buffer overflow in WebKit in Apple Safari before 4.0.3 allows remote attackers to execute arbitrary code or cause a deni service (application crash) via crafted floating-point numbers.
Published: 08/12/2009
CVSS Severity: 9.3 (HIGH)
CVE-2009-2494
Summary: The Active Template Library (ATL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via vectors related to erroneous free operations af reading a variant from a stream and deleting this variant, aka "ATL Object Type Mismatch Vulnerability."
Published: 08/12/2009
CVSS Severity: 10.0 (HIGH)

(그림 2-7) CVE 항목대상 CVSS 측정 예

중 2009년도에 보고된 취약점 항목의 일부 내용이다.

(그림 2-8)은 년도 별로 전체 취약점을 CVSS 기본 점수에 따라 심각도 High, Medium, Low로 분류된 취약점의 개수와 비율을 나타낸다.

Statistical Data

Year	# of Vulns	% of Total
2005	2,043	41.41
2006	2,756	41.71
2007	3,161	48.53
2008	2,846	50.53
2009	1,693	45.07

Statistical Data

Year	# of Vulns	% of Total
2005	2,437	49.40
2006	3,337	50.50
2007	3,122	47.93
2008	2,606	46.27
2009	1,721	45.82

Statistical Data

Year	# of Vulns	% of Total
2005	453	9.18
2006	515	7.79
2007	231	3.55
2008	180	3.20
2009	118	3.14

(그림 2-8) CVSS 기본점수: High / Medium / Low

2. OSVDB(Open Source Vulnerability DataBase)

오픈 소스 취약점 데이터베이스(OSVDB) 프로젝트는 전 세계 정보 보안 커뮤니티에서 자유롭게 사용할 수 있도록 컴퓨터의 보안 취약점 모음을 관리한다. 모아진 보안 취약점들은 운영체제, 소프트웨어, 프로토콜, 하드웨어 장치 그리고 다른 정보 기술 인프라의 요소들에서 알려진 보안 취약점에 대한 정보를 포함하고 있다. OSVDB 프로젝트는 인터넷 상에서 오픈 소스 취약점들을 모으고 이 취약점 데이터베이스 정보를 많은 커뮤니티에 제공하기 위한 프로젝트이다.

이 프로젝트가 어려운 이유는 취약점을 문서화하고 전파하는 것이 엄청난 작업이기 때문이다. CERT 취약점은 1995년에는 불과 200건 이하의 취약점이 발견되었지만 2003년에는 3,784건이 보고되었다. 즉, 7년 동안 2000%이상 증가하였다. CERT의 취약점 수은 보수적인 추정치이며 관리자, 개발자 및 기업들이 직면한 취약점의 실제 수는 실제로 훨씬 더 높을 수 있다.

취약점을 추적하는 데 필요한 노력은 대부분 조직의 자원을 초과하고, 매년 나타나는 정보의 양은 방대하다. 취약점 관리에 대한 증가하는 요구를 충족하기 위해, OSVDB은 세계의 보안 실무자의 노력 및 오픈 소

스 개발 모델의 위치, 검증, 중요한 정보의 문서화를 활용할 계획이다. OSVDB 프로젝트는 리눅스와 아파치 프로젝트와 같이 그 분야에서 선도적인 오픈 소스 프로젝트가 될 것을 목표로 하고 있다. 보안 커뮤니티와 밀접한 관계를 유지함으로써, 상업적 이익 및 상업적 커뮤니티 콘텐츠 개발하는 것에 대해 독립적으로 기관을 유지하며, 적극적으로 운영의 우수성을 홍보하여, 모든 보안 프로젝트와 실무자를 위한 세계적 수준의 자원에 대하여 OSVDB는 안정성을 제공할 것이다.

OSVDB 프로젝트는 2002년에 시작되었다. 지금까지의 많은 취약점 데이터베이스들이 있어왔으며 이러한 데이터베이스들은 주로 그들 자신의 요구를 만족시키기 위한 것이고. 어떤 것들은 한정된 취약점 집합만을 포함하고 있거나 내용에 중요한 제한을 가지고 있다. OSVDB 취약점 데이터베이스는 포괄적이고, 무료사용으로 개방하고, 사회의 요구에 부응하기 위해 만들어졌다. OSVDB는 현재 93,152 개의 취약점을 데이터베이스화 하고 있다.

OSVDB는 현재 활성화된 www.OSVDB.org에서 이용할 수 있다. 이것은 크게 두 부분으로 구성되는데 “프런트 엔드”는 취약점을 검색하고 리포트하기 위한 것이고, “백 엔드”는 취약점들을 추가하고 수정하기 위한 것이다.

OSVDB 조정자는 새로운 취약점들을 확인하고 그것들을 개인적인 기고자나 OSVDB “맹글러(mangler)”에게 할당한다. 맹글러는 취약점을 묘사하는 정보를 얻기 위해 웹을 샅샅이 뒤지고 OSVDB 내부의 데이터베이스 정보에 세부사항을 조사한다. 조정자는 그것을 승인하기 전에 명확성과 정확성을 요구하는 OSVDB의 표준에 적합한지 확인하기 위해 각각의 취약점 엔트리를 확인한다. 취약점의 해당 레코드가 받아들여지면, 데이터베이스화 되며 취약점 정보를 요청하는 누구나 이용가능하다. 이 과정은 빠르게 진행되어 커뮤니티에서 이용할 수 있는 취약점들을 만들어낸다. 이러한 과정은 맹글러와 조정자의 생산력을 최대화시키고, 따라서 취약점 데이터 증가를 안정적으로 유지할 수 있다.

3. CNVD (China National Vulnerability Database)

가. 목적 및 대상

CNVD (China National Vulnerability Database)는 2009년 구축된 중국내 취약점 데이터베이스로 보안제품 인증 평가기관인 CNITSEC에 의해 운영되고 있다. 2010년 4월부터 약 27,000개의 취약점 정보를 구축하여 서비스를 시작하고 있으며, 현재 40,000개 이상의 CNVDB 엔트리, 80,000개 이상의 패치와 수정 정보를 담고 있다. CNCERT/CC 사무국을 중심으로 중국 ISP, 네트워크 보안 회사들과 소프트웨어 회사 및 인터넷 회사들이 포함되어있는 CNVD는 300명이 넘는 중국내 화이트해커, 소프트웨어, 디바이스 제품을 판매하는 200개 이상의 회사, 그리고 24명의 멤버들이 기술적인 협력을 통해 운영 중이다.

CNVD는 회사에게는 경고 서비스와 기술적인 지원을, 공공기관에게는 끊임없이 추적한 버그 수정과 신뢰할 수 있는 취약점 정보 공개를, 사용자에게는 취약점에 초점을 둔 리스트 업데이트를 목적으로 한다.

CNVD 취약점은 미국의 NVD, 일본의 JVN 등과 유사한 형태의 정보 서비스를 제공한다. CNVD는 중국내 사용자들에게 중요한 영향을 미치는 취약점을 7개 카테고리로 구분하여 관리한다.

- o 일반 소프트웨어
- o 웹 응용
- o 운영체제
- o 데이터베이스
- o 네트워크 장치
- o 보안 제품
- o 산업용 소프트웨어(통신, 모바일 인터넷, 산업용 제어 시스템)

(그림 2-9) CNVD 홈페이지

나. 등록 방법

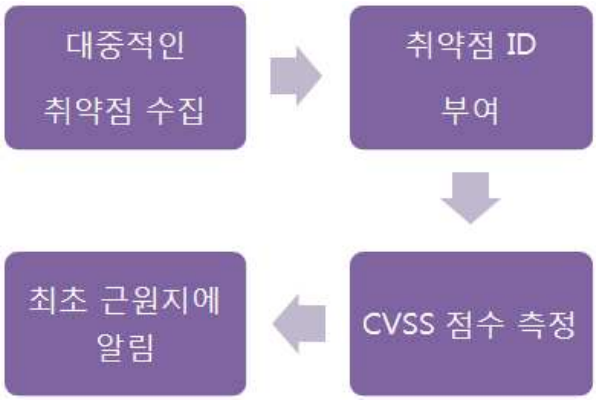
CNVD에서의 취약점을 등록 절차는 회원가입 후 인증된 사용자만이 가능하며, (그림 12)와 같이 메뉴 클릭을 통해서 접수 등록된다. 현재 등록된 CNVD에 등록된 ID 총 개수는 다음과 같다.

o CNVD ID 총 개수 : 81,884
o CVE ID : 42,857
o BUGTRAQ ID : 21,641

CNVD의 등록은 공개(public) 등록과 비공식적(private)인 등록 과정으로 구분되어 진해된다. 공개 등록의 경우 많은 소스들로부터 대중적인 취약점을 수집하는 것을 목표로 한다. 공개 등록의 경우 다음의 과정을

거쳐 수행된다.

o CVE ID, BID 또는 다른 공식적인 협회의 취약점 ID를 부여한다
o 유효한 것으로 간주하고 CVSS 점수를 측정한다
o 최초의 참조자(신고자)들에게 발표한다.



(그림 2-10) 대중적인 취약점 처리 프로세스

반면에 비공식적인 취약점 처리 프로세스는 취약점 등록을 위해 사용자 인증 절차를 거쳐서 사용자 등록이 완료되며, 취약점 등록은 사용자 정보 입력 후 이메일 인증을 통해서 사용자 인증이 이루어진다.

취약점 등록시 입력사항은 다음과 같다.

1) CNVD ID 스키마 형태
CNVD-YYYY-NNNNN (ex. CNVD-2013-26522)

2) CNVD 취약점 보고 내용
제목, CNVD ID, CVE ID, BUGTRAQ ID, 시간, 위험 레벨, 기본 설명, 참조 URLs, 제품, 해결책, 판매사 패치들과 다른 정보

(그림 2-11) CNVD 취약점 처리 프로세스

(그림 2-12) CNVD 홈페이지에서 취약점 제출 화면

3) 기본 설명

o 제품 설명(which)

o 취약 지점(where)

o 기술적인 분석과 설명(how)

o 효과와 위험 설명(what)

다음은 CNVD를 통해 등록된 취약점 중 Adobe Flash Player / AIR Unspecified Memory Corruption Vulnerability에 관련된 내용을 소개한 것이다.

(그림 2-13) CNVD의 취약점 보고 예시

다. 관련 사이트

o http://www.cnvd.org.cn/

o http://sbin.cn/blog/2009/10/19/china-national-vulnerability-database-gets-online/

제 4 절 국내외 취약점 포상 사례

본 절에서는 취약점 포상과 관련한 국내외의 대표적인 사례를 중심으로 포상 프로그램의 구성과 특징을 소개한다. 사례 분석의 대상으로 국외의 경우 마이크로소프트, 구글, 페이스북, 어베스트, 모질라, 시큐니아, 중국의 CNVD, 티핑포인트사 등 8개 사의 포상 프로그램을, 국내 경우로는 한국인터넷진흥원의 포상 프로그램의 구성을 살펴본다.

1. 마이크로소프트 BlueHat Prize

가. 목적 및 대상

마이크로소프트사는 자사의 프로그램을 대상으로 하는 사이버 공격 범죄가 증가함에 따라 컴퓨터 보안 방어기술에 대한 연구를 장려를 목적으로 시상 프로그램을 마련하였다. 2011년 8월 첫 해의 블루햇 프라이즈에서는 총 20건의 보안 아이디어가 접수됐으며, 블랙햇 보안 컨퍼런스 이전까지 접수된 아이디어에 대한 평가를 마치고 우승자를 선정하였다. 마이크로소프트사 입장에서 블루햇 프라이즈를 운영하는 것은 경제적인 방법으로 새로운 보안 아이디어를 확보하는데 목적이 있다고 할 수 있다. 블루햇 프라이즈는 버그 헌팅의 결과로 이에 대한 보상을 하는 일반적인 보상 프로그램과는 달리 참여자들로 하여금 보안 문제 해결에 관한 획기적인 기술을 창안해 내는 것을 목적으로 한다. 예를 들어 이 프로그램

을 통해 발견된 ROP 버그는 ASLR(Address Space Layout Randomization) 같은 기존 윈도우의 취약점 보호 기술을 우회하는 데 사용할 수 있는 것으로 알려졌다.

나. 포상기준 및 금액

- o 이 프로그램은 1등 $200,000, 2등 $50,000을, 3등은 MSDN 구독권을 지급하며, 총 상금은 26만 8천달러로 책정되었다.
- o 2011년도 블루햇 프라이즈의 경우 20개의 아이디어에 대해 26만 달러 가량이 지출된 것을 볼 때 절반 정도의 아이디어가 겹친다는 가정을 하면 하나의 아이디어당 2만 7천 달러가 지급되었다.
- o 윈도우 애플리케이션의 메모리 보안 취약성을 악용하는 것을 예방하는 가장 혁신적인 프로토타입을 개발한 사람에게 제공한다.

다. 기타 사항

- o 우승자는 그 해 블랙햇 보안 컨퍼런스에서 발표되며, 우승자는 물론 모든 대회 참가자는 자신들이 개발 기술에 대한 지적재산권을 가지지만, 마이크로소프트에는 로열티 없이 해당 기술을 라이센싱하는 조건이다.
- o 신청은 2MB 이하의 윈도우 SDK를 사용해 개발하고 윈도우에서 구동하는 2MB 이하 크기의 프로토타입을 제공해야 한다.
- o 이 프로그램을 통해 마이크로소프트사는 22개의 패치되지 않은 취약점을 찾았다. 이 중 5개는 Microsoft Office 제품군에서 존재(4개는 엑셀, 1개는 파워포인트)하는 것으로 보고되었다.

라. 참고 사이트

o http://www.itworld.co.kr/news/75108
o http://mbn.mk.co.kr/pages/news/newsView.php?category=mbn00008&news_seq_no=1092069
o http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=0005197212
o http://techtalk.seattle.gov/2011/02/10/microsoft-bug-bounty-program-reveals-22-unpatched-flaws-5-in-office/

2. 마이크로소프트 Catch Worm Creator

가. 목적 및 대상

Catch Worm Creator 프로그램은 전 세계적 윈도우 사용자들에게 바이러스와 유사한 문제를 일으키는 PC 바이러스 제작자와 유포자를 지역이나 국가와 관계없이 체포할 수 있도록 하는 제보 수집 프로그램으로 출발하였다. 이 프로그램은 보안 아이디어를 찾거나, 보안 취약점의 신고를 받는 기존의 보상 프로그램과는 다른 바이러스 제보자 색출이 목적인 프로그램이다.

나. 포상기준 및 금액

초기에 시행된 이 프로그램의 결과 $25,000의 포상금이 지급되었다.

다. 기타 사항

o 이 프로그램은 24시간 내에 200만 PC를 감염시킨 악명 높은 Conficker 혹은 Downadup virus의 출현으로 인해 시행되었다.
o 콘피커(Conficker)는 2008년 10월부터 확산되기 시작한 컴퓨터 웜으

로 다운업(Downup), 다운애드업(Downadup), 키도(Kido)라는 이름으로도 알려져 있다.

- o 콘피커 웜은 윈도 2000, 윈도 XP, 윈도 비스타, 윈도 서버 2003, 윈도 서버 2008의 윈도 서버 서비스의 취약점을 이용해 공격한다.
- o 콘피커가 등장한 이후 여러 변종 웜이 추가적으로 발견 되었으며, 이 중 콘피커.A (Conficker.A)는 2008년 11월 21일에, 콘피커.B는 2008년 12월 29일, 콘피커.C는 2009년 2월 20일에 발견되었으며 이후 콘피커.D, 콘피커.E는 2009년 4월 7일에 발견되었다.
- o 콘피커는 컴퓨터에서 실행되었을 때 윈도 자동 업데이트, 윈도 관리 센터, 윈도 디펜더, 윈도 오류 보고 같은 시스템 서비스 몇 개를 비활성화시킴. 그런 다음 서버에 연결해 추가로 전파할 명령을 받고, 개인 정보를 전송하고, 숙주가 된 컴퓨터에 맬웨어를 다운로드해 설치. 또한 이 웜은 svchost.exe, explorer.exe, services.exe 같은 중요한 윈도 프로세스에도 감염시켰다.

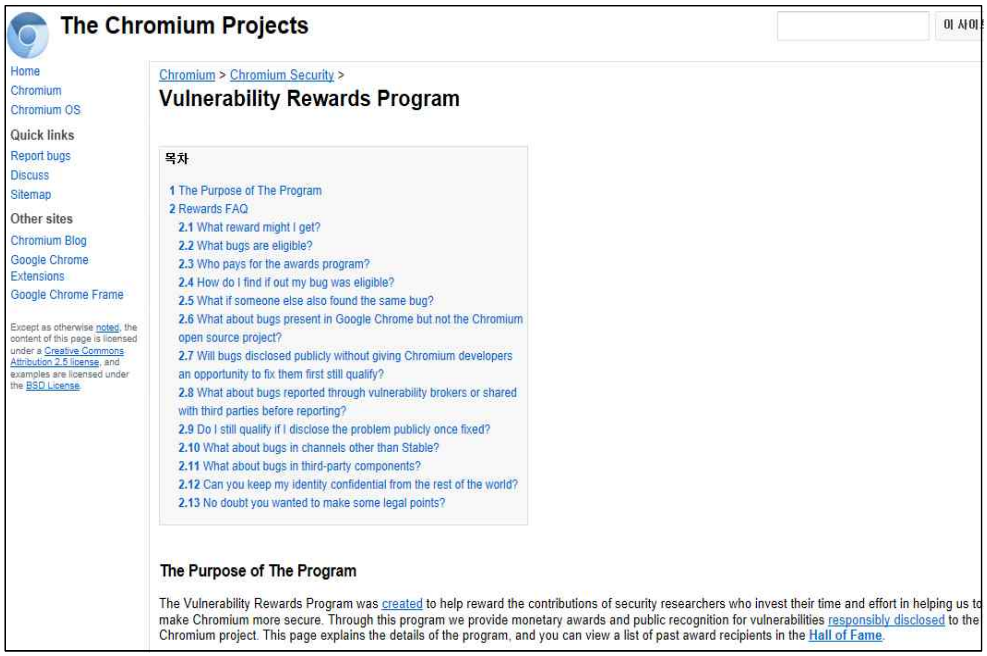
라. 참고사이트

- o http://www.rizwanashraf.com/2009/02/15/microsoft%c2%b4s-250000-reward-to-catch-worm-creator/
- o http://ko.wikipedia.org/wiki/%EC%BD%98%ED%94%BC%EC%BB%A4

3. 구글 Chromium Projects내의 Vulnerability Rewards Program

가. 목적 및 대상

구글의 웹 브라우저인 Chromium의 보안성 강화를 목표로 구글 브라우저에 국한된 보안 약점 수집을 목표로 시작하였다.



(그림 2-14) 크롬 프로젝트

나. 포상기준 및 금액

구글 Vulnerability Rewards Program은 취약점의 종류에 따라, 그리고 그 파급영향에 따라 다음과 같은 포상 금액을 책정하여 차별화 한다.

[표 2-21] 구글의 보상프로그램 등급

	구글 계정관련	다른 민감한 서비스	우선순위가 낮은 사이트
원격 코드 실행	$ 20,000	$ 20,000	$1,337- $5,000
SQL 주입 또는 동급	$ 10,000	$ 10,000	$1,337- $5,000
중요한 인증 우회 또는 정보 누출	$ 10,000	$ 5,000	$ 500

일반적인 XSS	$ 3,133	$ 1,337	$ 100
XSRF, XSSI 및 기타 일반적인 웹 취약점	$500~ $3,133	$500~$1,337	$ 100

다. 특징 사항

이 프로그램은 보상이 지급되는 버그 수준을 다음과 같은 세 가지 수준으로 구분한다.

(1) 매우 심각한 위험 (Critical Severity)

공격자가 검색의 정상적인 과정에서 사용자의 권한으로 임의의 코드를 실행할 수 있다. 이 수준에 해당하는 위험의 예는 다음과 같다.

- o 브라우저 프로세스의 통제 버퍼 오버플로우, 특히 악의적인 웹 사이트가 직접 버퍼의 내용을 제어할 수 있는 경우.
- o 브라우저 프로세스에서 대부분의 메모리 안전 문제가 되지 않는 임의의 코드 실행의 가능성을 배제 할 수 있음.
- o 모든 충돌은 중요한 취약점을 나타냄. 크롬은 메모리가 모두 다른 예외적인 상황에 있을 때 (예를 들어, debug break를 포함) 제어 방식으로 충돌하도록 설계되어 있음.
- o 특별한 사용자 작업을 필요로 하는 임의의 코드 실행 취약점(예 : 인증서 오류 메시지를 인쇄하거나 특정 명령 줄 플래그와 함께 크롬을 실행하는 것) 이 일반적으로 중요한 것으로 평가되어서는 안됨.

(2) 고수준의 위험 (High Severity)

공격자가 다른 웹 사이트에 속하는 기밀 데이터를 읽거나 수정할 수 있다. 이 수준에 해당하는 위험의 예는 다음과 같다.

- o 버그가 동일 출처 정책을 우회 할 수 있음
- o 샌드 박스의 범위 내에서 버그는 임의의 코드 실행을 허용
- o 버그가 브라우저의 보안 기능을 방해함. 예를 들면 버그는 위치 표시 줄 및 잠금 아이콘을 방해함 (상태 거품은 보안 표시가 아님.)

(3) 중간 수준의 위험 (Medium Severity)

공격자가 제한된 양의 정보를 얻을 수 있다. 이 수준에 해당하는 위험의 예는 다음과 같다.

- o 버그는 공격자가 최근에 방문한 URL을 열거 할 수 있도록 함
- o 버그는 독립적으로 유해하지 않음, 하지만 해를 입힐 다른 버그와 결합 할 수 있음. 예를 들어, "do not cache" 지시문을 무시하는 것 자체는 해롭지 않을 수도 있지만 다른 공격을 용이하게 할 수 있음
- o 높은 위험이 될 수 있는 버그가 아니더라도 특별한 사용자 작업이 필요함 (예 : 전체 화면 모드에서 탭의 프로세스를 종료 등)

(4) 낮은 수준의 위험 (Low Severity)

중요하지 않은 브라우저 기능을 통해 침입자가 일시적으로 제어 할 수 있다. 이 수준에 해당하는 위험의 예는 다음과 같다.

- o 버그는 공격자가 브라우저를 중지 할 수 있도록 함. (탭을 닫는 것만으로 해결 될 수 있는 경우 탭 정지는 보안 문제가 되지 않음.)

라. 등록 방법

구글 Vulnerability Rewards Program은 취약점 등록과 버그 등록을 구분한다. 취약점 등록은 구글 웹 사이트를 통해 제공되는 보안 템플릿을 통해 등록한다. 취약점 등록 과정을 살펴보면 다음과 같다.

- o 명확하고 기술적인 제목을 포함하여야 한다.
- o 크롬 /크롬버전 번호 및 릴리스 채널을 포함한다.
- o 운영 체제,버전 및 테스트 플랫폼의 서비스 팩 수준을 나열한다.
- o 크롬에 로드할 때 버그를 재생산한 HTML또는 이진파일이 첨부 된 버그의 데모를 포함한다.
- o 가능한 한 작게 파일을 만들고 취약점을 악용하는 데 불필요한 내용을 제거한다.
- o jQuery나 프로토타입 같은 타사 라이브러리에 대한 종속성을 피한다.
- o 15 줄 가량의 짧은 설명이나 HTML과 같은 텍스트기반의 테그, 그리고 텍스트 형식의 재현 케이스를 직접 포함한다.
- o 재현하는 데 필요한 자세한 내용과 함께 버그의 성격에 대한 간단한 설명을 제공한다.
- o 불필요한 주석이나 과장을 피한다.

취약점 보고 템플릿의 구성은 다음과 같다.

- o 취약점 세부 정보 : 보안 문제에 대한 간략한 설명을 제공함
- o 버전 정보 형식
  - ◆ Chrome Version: [x.x.x.x] + [stable, beta, or dev]
- o 운영체제 형식

- OS 버전, 서비스 팩 수준 등

o 크롬에서 로드할 때 버그를 생산한 HTML또는 이진파일과 같은 보안 버그의 데모를 포함
  - Type of crash: [tab, browser, etc.]
  - Crash State:[see link above: stack trace, registers, exception record]
  - Client ID (if relevant): [see link above]

구글은 보안 취약점과는 다른 범주로 크래쉬 버그(crash bug)에 대한 리포팅을 별도로 받고 있다. 크래쉬 버그는 다음과 같은 과정을 통해 보고된다.

o 브라우저(응용 프로그램 충돌) 또는 sad tab에서 충돌의 여부를 확인한다.
o 예외 세부사항 버그 설명서, 레지스터 상태와 스택 추적의 적절한 부분에 붙여넣기를 한다.
o 플랫폼 특정 디버거 구성은 윈도우, 맥 OSX, 리눅스 상에서 작동되는 것으로 한다
o 충돌보고를 사용하는 경우, 클라이언트 ID를 제공한다.
o 가능한 한 충돌에 대한 정확한 재현 단계 표현한다.
o 좀 더 많은 디버깅 정보를 제공한다.
o 가능하다면 구글에서 제공하는 구글 크롬 설정의 충돌 보고를 사용한다. 이 경우 chrome://chrome/settings로 이동하여 “Show adnanced settings”를 클릭하고, 개인 정보 섹션에서 "자동으로 Google로 사용 통계 및 충돌 보고서를 보냄"을 선택 한다.

마. 관련 사이트

- http://www.chromium.org/Home/chromium-security/vulnerability-rewards-program
- http://www.chromium.org/Home/chromium-security/reporting-security

4. 어베스트(Avast) Bug Bounty

가. 목적 및 대상

어베스트사의 보상 프로그램은 보안소프트웨어를 대상으로 한다는 점에서 브라우저나 운영체제 등 다른 프로그램에 대한 취약점을 찾는 보상 프로그램 차별화된다. 보안 소프트웨어라고해서 다른 프로그램보다 보안 문제에 자유로울 것이라 생각할 수 있지만 실제는 그렇지 않다. 오히려 보안 소프트웨어는 공격자에게 더 노출될 수 있다는 위기감이 어베스트사의 보상 프로그램을 탄생시킨 배경이 된다. 이를 통해 보안 프로그램 상의 버그를 발견하고 수정하기 위해 사용자 커뮤니티를 이용하는 것이 일반적으로 그렇지 않은 기업보다 더 성공할 수 있을 것이라는 것이 어베스트사의 시각이다.

나. 포상기준 및 금액

제보자에게는 각 전문가 패널에 의해 판단된 버그의 중요성에 따라 버그 당 최소 200달러가 지급되며, 원격코드 실행과 관련한 버그에는 3,000~5,000달러의 보상금이 지급된다.

다. 시행 방법

(그림 2-15) 어베스트사 버그바운티

보안 프로그램 대상 제품을 대상으로 하며, 어베스트사의 최신 버전 소프트웨어들로 윈도우 버전의 Avast제품 사용자에게만 국한된다.

o Avast 무료 안티바이러스(Avast Free Antivirus)
o Avast 프로 안티바이러스(Avast Pro Antivirus)
o Avast 인터넷 시큐리티(Avast Internet Security)

보고되는 보안 문제는 다음과 같은 순서로 위험성이 분류된다.

o 원격 코드 실행 (Remote code execution) : 가장 치명적
o 로컬 권한 상승 버그 (Local privilege escalation) : admin 계정이 아닌 계정에서 admin 권한을 얻을 수 있는 버그
o 서비스거부 취약성 : AvastSvc.exe 프로세스의 실행을 통해 발생할 수있는 BSOD나 시스템 크래쉬의 경우에 해당함
o Avast 샌드박스 우회 혹은 회피 가능 버그
o 스캐너 우회 침입

라. 취약점 보고 방법

- o Avast가 해당 버그를 확실하게 재현할 수 있을 정도의 충분한 정보가 포함된 보고서를 제출해야 함. 이 때 정확한 환경, 자세한 버그 설명, 샘플 코드 등 관계있는 모든 정보를 포함해야 한다.
- o 작성한 보고서를 이메일(bugs@avast.com)로 보내어 버그를 보고 함. 이 메일을 암호화하고 싶은 경우 PGP key를 사용한다.

마. 기타 특징 사항

- o AVAST와 그들의 가까운 친척 (부모, 형제, 자매, 자녀, 또는 배우자)와 AVAST 비즈니스 파트너, 정부 기관, 유통 업체, 그리고 직원들은 이 프로그램에서 제외한다.
- o 두 명 이상의 연구자가 동일한 버그를 발견하는 일이 있다면, 보상금은 먼저 제출한 사람에게 지급된다.
- o 제기된 문제가 수정된 후에 보상금이 지급된다.

바. 참고 사이트

- o http://www.boannews.com/media/view.asp?idx=34618&kind=1
- o http://blog.avast.com/2013/01/25/introducing-avast-bug-bounty

5. 페이스북(Facebook) Bug Bounty(2012)

가. 목적 및 대상

페이스북은 750 개 이상 만 명의 사용자를 가지고 있기 때문에 취약점이 잠재적으로 사람들의 거대한 숫자에 영향을 미칠 수 있으므로

Security Bug Bounty Program을 통해 해커가 취약점을 찾도록 하여 웹 사이트에 긍정적인 영향을 줄 목적으로 시행되었다.

나. 포상기준 및 금액

- o 최저 보상은 500 달러에서부터 시작된다.
- o 각각의 버그는 그 심각성과 창의력에 따라 보상이 수여된다.
- o 보안 버그 하나 당 한 번의 보상이 수여된다.

다. 시행 방법

- o 책임감 공시 규정(Responsible Disclosure Policy)에 준거한다.
- o 버그를 공개하는 최초의 사람에게 지급된다.
- o 페이스북 사용자 데이터의 무결성을 손상시킬 수 있는 버그나 페이스북 사용자 데이터의 개인 정보 보호를 회피하거나 Facebook의 인프라 내에서 시스템에 액세스 할 수 있도록 하는 등의 오류를 보고한다.

이러한 범주의 오류는 다음과 같다.

- o 크로스사이트 스크립팅 (XSS)
- o 크로스사이트 요청위조 (CSRF / XSRF)
- o 인증 오류 (Facebook의 OAuth 버그 포함) (Broken Authentication)
- o 플랫폼 / 개인 정보 보호 권한 모델 우회
- o 원격 코드 실행 문제점 (Remote Code Execution)
- o 권한 상승 (Privilege Escalation)
- o 프로비저닝 오류 (Provisioning Errors)

라. 기타 특징 사항

보상의 대상이 되지 않는 버그 종류는 다음과 같은 것이 있다.

- o 타사 응용 프로그램의 보안 버그
- o Facebook과 통합 타사 Web 사이트의 보안 버그
- o DoS 취약점
- o 스팸 또는 사회 공학 기법의 공격

마. 관련 사이트

- o http://www.h-online.com/security/news/item/A-5-000-vulnerability-in-Facebook-1673573.html
- o https://www.facebook.com/whitehat/

6. 모질라(Mozilla) Bug Bounty Program

가. 목적 및 대상

모질라의 버그 보상 프로그램은 모질라 소프트웨어의 보안 연구를 장려하고 좀 더 안전한 인터넷 클라이언트를 만드는 데 도움이 된 사람들에게 보상하기 위해 설계되었다. 보안 프로그램 대상은 Aurora, Beta or EarlyBird, and nightly mozilla-central releases 등 최근의 주요 개발 프로그램 또는 Firefox, Thunderbird, Firefox for Android 혹은 Mozilla Corporation에 의해 발표된 Mozilla서비스를 포함한다.

나. 포상기준 및 금액

o Client Reward Guidelines에 의하면 유효한 중요한 클라이언트 보안 버그 보상은 $3000의 현금 보상과 모질라 T 셔츠를 제공함
o Web Application and Services Reward Guidelines에 의하면 유효한 웹 응용 프로그램이나 보안 버그 관련 서비스에 대한 보상은 높은 심각도이거나, 어떤 경우에는, 특별한 또는 중요한 취약점은 $ 3000 (미국)까지 지불한다. 보통 $500에서 시작 하며 모질라 T-셔츠를 포함한다.

다. 시행 방법

모질라 취약점 포상 가이드라인에서는 다음 사항을 규정하고 있다.

o 버그는 이전에 보고되지 않은 최초의 버그여야 한다.
o 버그는 원격 공격(remote exploit)되는 형태이어야 한다.
o 제출자는 Mozilla 프로젝트에 참여하지 않은 사람이어야 하며, 버그 코드의 저자여서는 안 된다.
o Mozilla재단이나 자회사의 직원은 지원할 수 있다.
o Mozilla 코드에서 급여를 받으면서 작업하는 중에 보안 버그를 발견한 경우에는 보상을 신청하지 않도록 하는 것을 권장한다.

라. 취약점 보고 방법

o 보안 버그를 설명하는 버그 보고서의 제출을 통해 취약점을 보고한다. ‘Proof of Concept’나 취약성을 증명하는 버그 리포트의 테스트 케이스나 링크를 첨부하는 것을 권장한다.
o 제출 한 버그 및 간단한 요약을 이메일로 Mozilla 보안 그룹에 통지한다.

마. 기타 특징 사항

- o 만일 두 연구자가 함께 버그를 보고하면 보상은 그들 사이에서 분할하여 지급된다.
- o 버그의 원인을 규명하고 수정하는데 Mozilla 엔지니어와 함께 작업할 수 있고 버그에 대한 내부 토론에 참여하는 권한을 제공한다.

바. 관련 사이트

- o http://news.blogsdna.com/13193/mozilla-reward-program-awards-12-year-old-bug-hunter.htm
- o http://www.mozilla.org/security/bug-bounty.html

7. 세큐니아(Secunia) SVCRP

가. 목적 및 대상

일반적으로 SW 벤더는 주요 취약점에만 보상을 주고 있으나 기타 취약점에는 소홀한 경향이 있다. 세큐니아 SVCRP (Secunia Vulnerability Coordination Reward Program)는 이를 보완하는 방법으로 비주류 취약점을 수집, 분석 후 벤더에게 리포팅한다. 세큐니아 SVCRP는 상용 패키지 (off-the-shelf) 제품을 대상으로 하며, 페이스북과 같은 온라인 서비스는 대상에서 제외한다.

나. 포상기준 및 금액

세큐니아 SVCRP는 주요 취약점의 수집을 목표로 하는 다른 보상 프로그램과는 달리 간과하기 쉬운 사소한 보안 취약점을 대상으로 한다.

따라서 포상 금액이나 지원 방식도 현금이 아닌 호텔 숙박권, 주요 보안 컨퍼런스 참가권을 지급한다.

다. 시행 방법

패키지 소프트웨어 벤더를 대신해 취약점을 수집하며, 대부분 제품의 모든 취약점 등급은 아래의 기준이 충족될 때 SVCRP에 적용 된다.

- o 취약점이 안정된 제품에 영향을 줄 경우
- o 취약점이 최신 버전의 제품에 영향을 줄 경우
- o 제품이 공급 업체(vendor)에 의해 지원 되는 경우
- o 이미 공개적으로 알려져 있지 않은 새로운 취약점인 경우

세큐니아 SVCRP를 통해서 연구결과에 맞게 연구원들에게 다음과 같은 구분을 통해 작은 보상이 수여된다.

- o Most Valued Contributor : Secunia Research의 판단에 따라 매년, 지속적으로 잘못된 부분을 교정하고 확인하기 쉽고 빠른 디테일한 취약점 보고서를 낸 연구자에게 수여됨
- o Most Interesting Coordination Report : Secunia Research의 판단에 따라 매년 가장 흥미로운 취약점을 제기한 연구자에게 수여됨 (기준의 예: 복잡성, impact, 영향을 받은 제품, 취약점 보고서의 세부 수준)

라. 취약점 보고 방법

- o SVCRP 통해 Secunia에 취약점을 보고하려면 '[SVCRP]'로 시작하는 취약점 보고서를 vuln@secunia.com으로 제출

o 보고서에는 제품/버전정보, Secunia Research가 조사 결과를 재현하기 위해, 취약점을 유발하는 세부적인 단계 혹은 PoC 또는 자세한 설명이 포함되어야 한다.

마. 기타사항

세큐니아사는 2013년 8월16일부로 SVCRP 프로그램의 종료를 선언하였다.

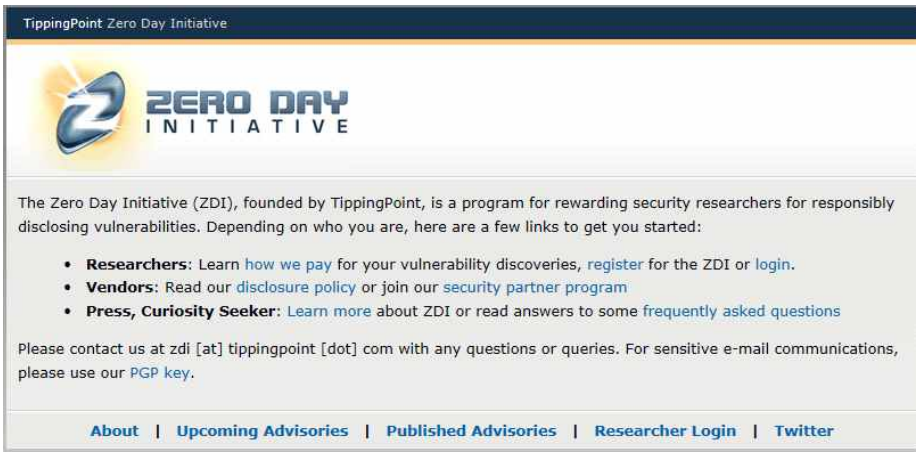
바. 관련 사이트

o http://secunia.com/community/research/svcrp

8. Zero Day Initiative

가. 목적 및 대상

제로데이 이니셔티브(www.zerodayinitiative.com)는 TippingPoint사에 의해 기획된 프로그램으로 취약점 발굴에 대한 보상 프로그램이다. Tipping Point 사는 보안 솔루션 회사로 2002년 침입방지시스템을 출시했으며, 제로데이 이니셔티브를 통해 보안문제에 대한 취약점 필터를 제공하고 있다.



(그림 2-16) 제로데이 이니셔티브 프로그램

나. 포상 기준 및 금액

제로데이 이니셔티브 프로그램은 보안전문가들을 대상으로 한 취약점은 다음과 같은 기준에 따라 차등을 두어 보상금이 지급된다.

- o 영향을 받는 제품은 얼마나 광범위한가?
- o 공격된 취약점으로 인해 어떤 수준의 권한이 침해받는가?
- o 취약점은 디폴트 설정이나 설치시 노출되어 있는가?
- o 영향을 받는 제품은 중요한 것에 속하는가? (예를 들면, 데이터베이스, 전자상거래서버, DNS, 라우터 방화벽 등)
- o 공격자는 일반 전문가(social engineer)들이 링크를 클릭함, 사이트를 방문함, 서버에 접속함 등으로 인해 희생자로 삼는가?

ZDI로 등록된 취약점과 관련하여 전문가에게는 항공 마일리지 개념과 유사하게 포인트가 부여된다, 포인트는 첫 번째 등록된 취약점에 대해 2,500 ZDI 포인트가 주어지며, 다음 수준별로 등급을 결정한다.

[표 2-22] ZDI 보상 등급

ZDI 보상포인트	등급
10,000	청동 ZDI
20,000	실버 ZDO
35,000	황금 ZDI
50,000	플래티넘 ZDI
75,000	다이아몬드 ZDI

등급별 상금 수준은 다음과 같다.

- 청동 ZDI
. 다음 연도에 모든 취약점 제출 10 % 자동 통화 보너스
. $1,000의 일회성 보너스

- 실버 ZDI은
. 다음 연도에 모든 취약점 제출 15 % 자동 통화 보너스
. 다음 연도에 모든 취약점 제출 25 % ZDI 보상 포인트 배율
. $5,000의 일회성 보너스
. 라스베이거스 DEFCON 컨퍼런스 참석을 위한 여행 및 등록경비

- 골드 ZDI
. 차년도 취약점 제출시 20 % 자동 통화 보너스
. 차년도 취약점 제출시 50 % ZDI 보상 포인트 배율
. $10,000의 일회성 보너스
. 라스베이거스 DEFCON 컨퍼런스 참석을 위한 여행 및 등록경비

- 플래티넘 ZDI
. 차년도 취약점 제출시 25 % 자동 통화 보너스
. 차년도 취약점 제출시 100 % ZDI 보상 포인트 배율

. $20,000의 일회성 보너스
. DEFCON 참석, 블랙 햇 컨퍼런스, 블랙 햇 교육 유료 등록 경비

- ZDI 다이아몬드 :
. 차년도 취약점 제출시 30 % 자동 통화 보너스
. 차년도 취약점 제출시 125 % ZDI 보상 포인트 배율
. $25,000의 일회성 보너스
. DEFCON 참석, 블랙 햇 컨퍼런스, 블랙 햇 교육 유료 등록 경비

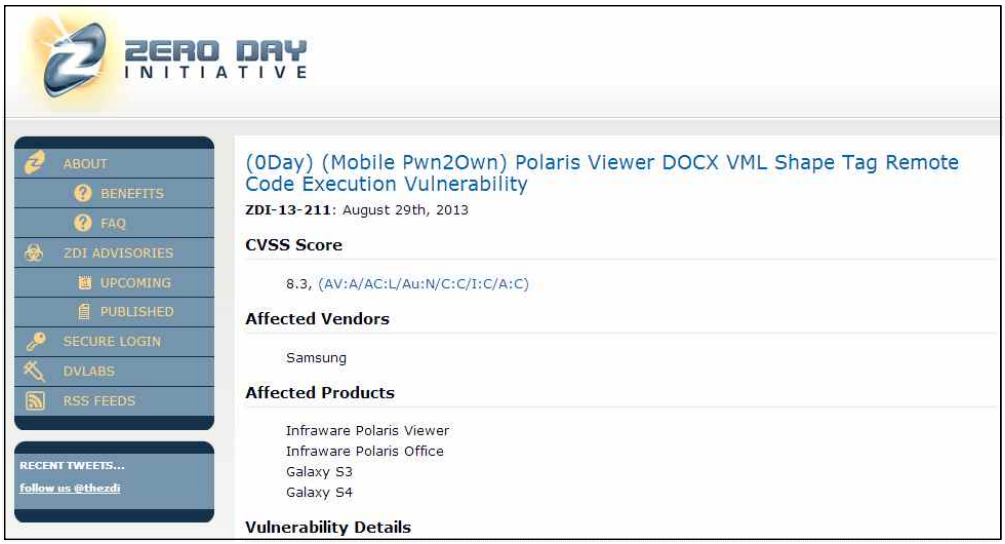
다. 특징 사항

이들 항목에 대해 보안 전문가들은 취약점 등록 시 항목별 평가를 함께 제출한다. 만일 등록된 취약점이 Zero day Initiative로 등록되어 보상금을 받지 못할 경우, 취약점에 대한 권리는 계속 발굴자에게 남는다.

라. 등록방법

제로데이 이니셔티브 프로그램에 등록한 전문가에 한해 제로데이 취약점 등록 시 다음 정보를 제공한다.

o 대상 제품
o 샘플 공격코드
o 취약점의 자세한 설명



(그림 2-17) 제로데이 이니셔티브 취약점 보고예시

최근 제로데이 이니셔티브에 보고된 삼성 모바일 디바이스의 취약점은 180일 데드라인 내에 삼성 측에서 특별한 응답을 하지 않은 관계로 8월 29일 다음과 같은 내용을 공개한 바가 있다.

(http://www.zerodayinitiative.com/advisories/ZDI-13-211/)

[표 2-23] 제로데이 이니셔티브 취약점 예

취약점명: Polaris Viewer DOCX VML Shape Tag Remote Code Execution Vulnerability	
ZDI 번호	ZDI-13-211
일시	August 29th, 2013
CVSS 점수	8.3, (AV:A/AC:L/Au:N/C:C/I:C/A:C)
피해 벤더	Samsung
피해 제품	Infraware Polaris Viewer, Infraware Polaris Office Galaxy S3, Galaxy S4

취약점 상세	이 취약점은 원격 공격자가 취약한 폴라리스 뷰어에서 임의 코드를 실행할 수 게 한다. 사용자는 악성 코드를 열어 실행함으로써 취약점이 발생한다. 결함은 DOCX 파일의 구문 내에 존재한다. VML과 관련된 태그가 제대로 검증되지 않았을 때 발생하며, 태그가 너무 큰 경우 오버 플로우가 인접한 버퍼에 발생한다. 이를 악용하여 공격자는이 메모리 제어 및 폴라리스 뷰어 응용 프로그램의 컨텍스트에서 원격 코드 실행을 보장 할 수 있다.
벤더 응답	완화방법: 사용자는 Samsung Galaxy S3 and S4의 문서를 열어보지 않음으로써 자신을 보호할 수 있다. Sept 19, 2012 - MWR Labs demonstrated an exploit against the Samsung Galaxy S3 running Android 4.0.4 at Mobile Pwn2Own 2012. Sept 20, 2012 - Samsung requested vulnerability information from ZDI. Sept 24, 2012 - ZDI requested contact information and PGP keys for secure communication of vulnerability information from Samsung. Sept 24, 2012 - Samsung provides ZDI with PGP and contact information. ... Mar 25, 2013 - 180 day deadline from vulnerability disclosure passes. ZDI able to disclose vulnerability as 0-day according to Vulnerability Disclosure Policy. Mar 25, 2013 - ZDI holds releasing advisory and waits for communication from Samsung. ... Aug 4, 2013 - ZDI notifies Samsung that Mobile Pwn2Own vulnerability will be disclosed as a 0-day before the end of August. Notification happened in person at DEF CON. Aug 5, 2013 - Samsung requests from ZDI via e-mail for more detail and a timeline of events associated with the vulnerability. Aug 7, 2013 - ZDI provides timeline and requests support. Aug 7, 2013 - Samsung states work with security@samsung.com to obtain vulnerability status update. Aug 8, 2013 - ZDI notifies Samsung (security@samsung.com, m.security@samsung.com) of impending 0-day disclosure. Aug 29, 2013 - No response from Samsung. ZDI discloses 0-day

	vulnerability advisory.
공개 일정	2012-09-26 - Initial contact with vendor 2013-08-29 - Public release of advisor This vulnerability is being disclosed publicly without a patch in accordance with the ZDI 180 day deadline.
Credit	This vulnerability was discovered by: MWR Labs

마. 관련 사이트

o http://www.zerodayinitiative.com

9. KISA SW 신규 보안 취약점 신고 포상제 (2012)

가. 목적 및 대상

KISA에서는 2006년부터 취약점 신고를 받아온데 이어, 2012년 10월부터는 우수 신규 취약점 신고에 대해 포상금을 지급하는 'S/W 신규 보안 취약점 신고 포상제'를 도입하였다. 해킹사고에 악용될 수 있는 취약점을 사전에 조치하고 관련 전문가의 취약점 발굴을 활성화하기 위한 목적으로 시작하였으며 통상 6개월에 20여건 미만이었던 신고 건수가 포상제 시행 후 60여 건으로 3배 급증하였다.

KISA의 SW 신규 보안 취약점 신고 포상제는 약점 신고 당시 보안 업데이트가 나오지 않은 취약점(제로데이 취약점)을 대상으로 하며, 서비스 운영 중인 홈페이지에 대해 공격 또는 모의해킹 수준으로 간주될 수 있는 취약점은 포상 및 평가 대상에서 제외한다. 이 경우 포상금 지급과 무관하게 신고는 가능하며, 검증 후에 해당 업체나 홈페이지 운영자에게 통보한다. 제로보드XE, 그누보드, 테크노트 등의 홈페이지 구축

소프트웨어도 포상 및 평가 대상에 포함한다.

나. 포상기준 및 금액

o 평가결과에 따라 최고 500만원이 지급되며 3, 6, 9, 12월등 일년에 4회에 걸쳐 취약점 평가 및 포상금이 지급된다.
o 포상 단위는 개별 신고건 단위로 지급된다.

다. 시행 방법

KISA 내부 및 외부의 취약점 전문가로 구성된 평가위원회에서 아래 평가 항목에 대해 취약점 평가된다. 평가 항목의 구성은 다음과 같다.
o 취약점 파급도(55점) : 취약점 발생 대상의 시장 점유율 및 위험도 등
o 취약점 기술 난이도(30점) : 취약점 동작 원리 및 구성의 난이도와 참신성
o 신고 내용의 완성도(15점) : 취약점 재연 방법의 정확성 및 취약점 테스트 환경 등에 대한 구체적인 기술 등

라. 취약점 보고 방법

인터넷침해대응센터 홈페이지 (http://www.krcert.or.kr)의 취약점 신고 페이지에서 신고양식을 다운로드받아 작성하여 관련파일에 첨부하여 제출한다. 신고양식을 이용하지 않을 경우 신고는 가능하나, 포상금 지급 대상에서 제외된다.

마. 기타 특징 사항

o KISA 인터넷침해대응센터 보안공지에서 해당 취약점에 대한 보안 업

데이트를 권고한다.

o 분석된 취약점은 해당 업체에 전달해 보안 업데이트를 개발하는데 사용되도록 한다.

바. 관련 사이트

o http://www.krcert.or.kr/kor/notice/noticeView.jsp?p_bulletin_writing_sequence=1403

o http://www.ittoday.co.kr/news/articleView.html?idxno=36249

제 3 장 CVSS 시범평가

제 1 절 CVSS 평가항목 및 평가기준

본 시범평가에서는 CVSS 평가 항목을 다음과 같은 6개의 범주로 재분류하였다.

- o 파급도
- o 기술적 영향
- o 시스템 중요도
- o 공격 난이도
- o 대응 난이도
- o 보고의 신뢰성

각 범주에 속한 CVSS 평가 항목의 평가 방법과 평가 기준은 다음과 같다.

1. 파급도

가. 대상 분포 (Target Distribution, TD)

- o 개요 : 이 평가항목은 보안 취약점으로 인해 침해가 예상되는 시스템의 범위를 평가하기 위하여 사용된다.

- o 평가방법 : 해당 취약점으로 인하여 영향을 받을 수 있는 시스템의 범위를 평가한다. 평가의 대상이 되는 시스템 환경이 달라짐에 평가 결과도 달라질 수 있다. 평가 대상이 되는 환경에서 침해가 예상되

는 시스템들의 범위가 넓을수록 높은 점수를 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	0.0	해당 보안 취약점으로 인하여 침해가 예상되는 시스템이 없거나 혹은 실험실 환경에서만 가능하여 실제적으로는 0%의 영향을 미치는 경우이다.
Low	L	0.3	해당 보안 취약점으로 인하여 침해가 예상되는 시스템 환경의 범위가 1% - 25%인 경우이다.
Medium	M	0.6	해당 보안 취약점으로 인하여 침해가 예상되는 시스템 환경의 범위가 26% - 75%인 경우이다.
High	H	1.0	해당 보안 취약점으로 인하여 침해가 예상되는 시스템 환경의 범위가 76% - 100%인 경우이다.
Not Defined	ND	0.0	이 값을 주면 취약성 점수에 영향을 주지 않는다.

2. 기술적 영향

가. 기밀성 영향 (Confidentiality Impact, C)

o 개요 : 이 평가항목은 취약점을 이용한 공격이 성공하였을 때 기밀성에 미치는 영향을 측정한다. 기밀성은 권한이 있는 사용자에게만 정보를 접근하여 볼 수 있도록 제한하여 권한이 없는 사용자가 정보를 접근하지 못하도록 하는 것이다.

o 평가방법 : 취약점 공격으로 발생 가능한 시스템의 정보에 대한 기밀성 침해 정도를 아래 표와 같이 None, Partial, Complete로 평가한다. 정보의 누출이 많을수록 기밀성 침해 정도가 큰 것으로 판단

한다. 기밀성 영향 값이 클수록 취약성 점수도 커진다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	0.0	시스템의 기밀성에 영향을 미치지 않는다.
Partial	P	0.275	상당한 정보의 누출이 있다. 몇몇의 시스템 파일에 대한 접근이 가능하다. 그러나 공격자는 획득한 것을 넘어 제어할 수는 없으며, 손실의 범위는 제한적이다. 예로서 DB에서 오직 일부 테이블만이 노출되는 취약점을 들 수 있다.
Complete	C	0.660	모든 시스템 파일을 드러내는 결과를 낳게 되는 완전한 정보의 누출이 있다. 공격자는 시스템의 모든 데이터를 읽을 수 있다.(메모리, 파일 등등)

나. 무결성 영향 (Integrity Impact, I)

o 개요 : 이 평가항목은 취약점을 이용한 공격이 성공하였을 때 무결성에 미치는 영향을 측정한다. 무결성은 정보 혹은 자료에 대한 신뢰도(trustworthiness)와 보증된 정확도를 나타낸다.

o 평가방법 : 취약점 공격으로 발생 가능한 시스템의 정보에 대한 무결성 침해 정도를 아래 표와 같이 None, Partial, Complete로 평가한다. 시스템 파일이나 정보의 변경 가능성이 클수록 또한 공격자가 변경된 정보를 마음대로 제어할 수 있을수록 무결성 침해 정도가 큰 것으로 판단한다. 무결성 영향 값이 클수록 취약성 점수도 커진다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	0.0	시스템 무결성에 대한 영향은 없다.
Partial	P	0.275	어떤 시스템 파일이나 정보의 변경이 가능하다. 그러나 공격자는 변경된 것을 제어할 수는 없거나 공격자가 영향을 미칠 수 있는 범위가 제한적이다. 예를 들어 공격자가 시스템이나 응용 파일을 덮어쓰거나 변경할 수는 있으나 영향을 받은 파일을 제어할 수 없거나 오직 제한된 범위 안에서만 변경할 수 있다.
Complete	C	0.660	시스템 무결성이 전체적으로 위험에 드러나 있다. 시스템 보호의 완전한 손실이 있으며, 이는 전체 시스템의 위험 노출로 이어진다. 공격자는 타겟 시스템이 어떤 파일에도 변경을 가할 수 있다.

다. 가용성 영향 (Availability Impact, A)

o 개요 : 이 평가항목은 취약점을 이용한 공격이 성공하였을 때 가용성에 미치는 영향을 측정한다. 가용성이란 정보 자원에 대한 접근과 사용을 의미한다.

o 평가방법 : 네트워크 대역폭, 프로세서 사이클, 디스크 공간 등을 소모시켜는 공격은 시스템 가용성에 영향을 준다. 취약점 공격으로 발생 가능한 시스템의 가용성 침해 정도를 아래 표와 같이 None, Partial, Complete로 평가한다. 시스템 성능 감소가 클수록 시스템 자원을 사용할 수 없을수록 가용성 침해 정도가 큰 것으로 판단한다. 가용성 영향 값이 클수록 취약성 점수도 커진다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	0.0	시스템의 가용성에 대한 영향은 없다.
Partial	P	0.275	성능이 줄어들거나 자원을 잠시 사용할 수 없게 된다. 하나의 예로 인터넷 서비스에 대한 연결 수에 제한을 두는 네트워크 기반의 플루드 공격을 들 수 있다.
Complete	C	0.660	영향을 받은 자원을 완전히 사용할 수 없게 된다. 공격자는 자원을 완전히 사용하지 못하도록 할 수 있다.

3. 시스템 중요도

가. 부수적 피해 잠재성(Collateral Damage Potential, CDP)

o 개요 : 이 평가항목은 취약점을 이용한 공격이 성공하였을 때 자산이나 장비의 파괴 혹은 도난으로 인해 발생할 수 있는 잠재적인 인적 물적 피해를 측정하며 이로 인해 발생할 수 있는 생산성이나 매출의 경제적 손실도 측정한다.

o 평가방법 : 취약점 공격으로 발생 가능한 물적 손실이나 자산 손실 혹은 기관의 생산성이나 매출에 대한 손실의 정도에 따라 아래 표와 같이 부수적 피해 잠재성 정도를 등급으로 정한다. 이 메트릭의 가능한 값들은 아래 표에 있으며 부수적 피해 잠재성이 클수록 취약성 점수는 커진다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	0.0	생명, 물적 자산, 생산성 혹은 매출에 대한 손실 가능성이 없다.
Low	L	0.1	약간의 물적 손실이나 자산 손실의 결과를 낳을 수 있다. 또한 기관의 생산성이나 매출에 약간의 손실이 있을 수 있다.
Low-Midium	LM	0.3	중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있다. 또한 기관의 생산성이나 매출에 중간 정도의 손실이 있을 수 있다.
Midium-High	MH	0.4	중요한 물적 손실이나 자산 손실의 결과를 낳을 수 있다. 또한 기관의 생산성이나 매출에 중요한 손실이 있을 수 있다.
High	H	0.5	재앙 수준의 물적 손실이나 자산 손실의 결과를 낳을 수 있다. 또한 기관의 생산성이나 매출에 재앙 수준의 손실이 있을 수 있다.
Not Defined	ND	0	이 값을 주면 취약성 점수에 영향을 주지 않는다.

나. 보안 요구조건(Security Requirements, CR, IR, AR)

o 개요 : 이 평가항목은 취약점 공격으로 영향을 받는 IT 자산의 사용자 환경에서의 기밀성, 무결성, 가용성의 중요도에 따라 CVSS 점수를 조정할 수 있도록 해준다. 즉, 기밀성, 무결성, 가용성의 중요도에 따라 기밀성, 무결성, 가용성 점수에 가중치를 줌으로써 취약성 점수를 조정한다.

o 평가방법 : 사용자 환경(기관이나 그 기관에 관계된 사람)에서 기밀성, 무결성,가용성의 상대적 중요도를 평가한다. [기밀성 | 무결성 | 가용성]의 손실이 사용자의 환경에게 끼치는 부정적인 영향이 클수

록 해당 보안 요구조건 이 큰 것으로 판단한다. 예를 들어 취약점 공격으로 영향을 받는 어떤 IT 자산이 가용성이 가장 중요한 비즈니스 기능을 지원하고 있다면 가용성에 상대적으로 더 큰 등급을 매길 수 있다. 각 보안 요구조건에 대해서 이 메트릭의 가능한 값들은 아래 표에 있으며 보안 요구조건이 클수록 취약성 점수도 커진다.

o 등급별 기준

등급	코드	점수	평가기준
Low	L	0.5	[기밀성 ¦ 무결성 ¦ 가용성]의 손실은 기관이나 그 기관에 관계된 개인(예. 직원, 고객)에게 제한적으로 부정적인 영향을 끼친다.
Midium	MH	1.0	[기밀성 ¦ 무결성 ¦ 가용성]의 손실은 기관이나 그 기관에 관계된 개인(예. 직원, 고객)에게 심각하게 부정적인 영향을 끼친다.
High	H	1.5	[기밀성 ¦ 무결성 ¦ 가용성]의 손실은 기관이나 그 기관에 관계된 개인(예. 직원, 고객)에게 재앙과 같은 부정적인 영향을 끼친다.
Not Defined	ND	1	이 값을 주면 취약성 점수에 영향을 주지 않는다.

4. 공격 난이도

가. 접근 벡터 (Access Vector)

o 개요 : 이 평가항목은 취약점을 통해 침해당하는 방법과 관련된 평가 척도로서, 원격의 접근을 통하여 침해가 가능할수록 높은 점수가 부여된다.

o 평가방법 : 취약점 공격을 위해 필요한 접근의 근접성을 기반으로 아래와 같이 Local, Adjeacent, Network로 분류한다. 공격에 필요한 접근 방법이 원격일수록 취약성 중요도 점수도 커진다. 여러 가지 접근 방법에 의하여 공격이 가능할 경우 가장 원격의 접근에 대응하는 가장 높은 점수를 부여한다. 또한 이메일 등으로 전달된 위험한 파일을 지역적인 응용프로그램의 사용하여 침해가 발생할 경우 공격자의 주요 행동을 기준으로 Network로 평가한다.

o 등급별 기준

등급	코드	점수	평가기준
Local	L	0.395	네트워크를 통한 접근이 아닌 호스트에 대한 직접 접근(Local Access)을 통해서 공격이 가능한 경우를 말한다. Firewall/USB 등의 DMA 공격이나, 지역 권한 상승(local privilege escalation) 공격 등이 이에 속한다.
Adjacent Network	A	0.646	IP 서브넷, 블루투스, IEEE 802.11, 로컬 이더넷 세그먼트 등을 통해서만 공격이 가능한 경우에 해당한다.
Network	N	1.0	L과 A에 해당하지 않는 경우로서, 일반적인 네트워크에 연결을 통하여 공격이 가능한 경우에 해당한다.

나. 접근 복잡도 (Access Complexity, AC)

o 개요 : 이 평가항목은 취약점을 가진 시스템에 접근이 가능한 상황에서, 침해에 필요한 과정의 복잡성을 평가한다. 과정이 복잡할수록 침해의 성공 가능성 또한 낮아지는 경향을 가지게 된다. 침해의 수행 이전에 위험한 파일의 설치와 같은 선행적인 침해가 필요한 경

우 High로 판정한다.

o 평가방법 : 취약점 공격으로 발생 가능한 시스템의 정보에 대한 무결성 침해 정도를 아래 표와 같이 High, Medium, Low로 평가한다.

o 등급별 기준

등급	코드	점수	평가기준
High	H	0.35	공격을 위한 다음의 예와 같은 특별한 조건을 요구한다. • 공격당하는 시스템 외에도 추가적인 시스템에 대한 상승된 권한의 획득이나 침해를 수행한다.(예. DNS hijacking) • 공격을 위해서 피해자에 대한 사회공학적인 방법에 의존하여야 한다. 이러한 방법은 보안에 대한 일정 지식을 가진 사람들에 대해서는 적용이 힘든 것이 일반적이다. 일반적으로 피해자가 위험할 수 있는 의심스러운 행동을 수행하여야 한다. • 취약한 환경이 실제적으로 잘 발생하지 않는다. • 경쟁 조건의 발생을 위한 기회가 매우 적다. • 위험한 파일의 설치와 같은 선행적인 침해가 필요하다.
Medium	M	0.61	다소 특별한 접근 조건을 요구한다. • 공격자가 일정 권한 수준에 해당하는 사용자 그룹 또는 사용자들로 제한되며, 신뢰되지 않는 그룹도 가능하다. • 공격 수행 전에 추가적인 정보가 수집되어야 한다. • 공격의 수행에 영향을 주는 환경이 기본 설정이 아니며, 일반적인 설정이 아니다. (예: 취약점은 서버가 특정 방법을 통해 사용자 계정 인증을 수행할 때 나타나지만 또 다른 인증 방법에서는 나타나지 않는다.) • 신중한 사용자를 속일 가능성이 있는 사회공학적인 방법을 사용하여야 한다. (예: 웹 브라우저의 상태 바를 다른 링크로 보이게 변경하는 피싱 공격.)

Low	L	0.71	특화된 접근 조건이나 환경은 존재하지 않는다. • 공격 대상 제품이 전형적으로 넓은 범위의 시스템과 사용자의 접근을 요구한다. • 공격 가능한 환경 설정이 기본 설정이며, 대부분 시스템에서 사용된다. • 공격자는 수동적으로 수행될 수 있으며, 추가적인 기법이나 부가적인 정보 수집을 거의 요구하지 않는다. • 경쟁 상황을 쉽게 발생시킬 수 있다.

다. 공격 가능성 (Exploitability)

o 개요 : 공격을 위한 방법이나 코드의 존재 여부를 기반으로 공격의 용이성을 평가한다.

o 평가방법 : 주어진 취약점에 대하여 해당 취약점을 공격하는데 사용되는 현재 기술의 수준에 따라 침해의 가능성은 크게 영향 받을 수 있다. 단순히 증명 코드만이 알려져 있거나, 활용 가능성이 있는 공격 코드가 발표된 경우, 확실한 공격 코드가 개발된 경우, 네트워크를 통하여 전파될 수 있는 공격 코드가 개발된 경우 등 침해에 사용될 수 있는 기술의 수준에 따라 취약점의 중요도는 영향을 받는다. 이를 고려하여 아래와 같은 기준에 따라 등급을 판정하며 복수에 해당할 경우 가장 높은 점수 등급을 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
Unproven	U	0.85	이용할 수 없는 공격 코드이거나 완전히 이론상으로 가능한 것이다.
Proof-of-concept	POC	0.9	공격의 개념을 시험하거나, 실제적으로는 대부분의 시스템에는 맞지 않는 공격 시연이 존재한다. 그 코드나 기술이 모든 환경에 적용되지 않으며, 숙련된 공격자에 의한 많은 변경을 필요로 한다.

Functional	F	0.95	기능적 공격코드가 이용가능하며 취약점이 발견된 대부분의 상황에서 영향을 미칠 수 있다.
High	H	1.0	각 취약점은 자발적으로 동작하는 모바일 코드에 의해 악용 가능하며, 또 직접적인 공격이 필요하지 않고, 침해 코드가 널리 이용가능하다. 코드는 모든 상황에서 영향을 미칠 수 있으며, 실질적으로 모바일 자발적인 에이전트(웜이나 바이러스 같은)를 통하여 전파 된다.
Not Defined	ND	1.0	본 메트릭은 점수에 영향을 미치지 않는다.

5. 대응 난이도

가. 대응 수준 (Remediation Level)

o 개요 : 대응 수준은 취약점에 대한 우선순위 설정을 위한 중요한 요소이다. 일반적으로 취약점이 발표될 시점에는 적절한 패치가 없는 경우가 많으며, 공식적인 패치나 업그레이드의 발표 이전에 비공식적인 회비 방법이나 수정이 발표되기도 한다. 이러한 대응의 단계에 따라 취약점에 대한 평가는 점차적으로 하향 조정될 수 있다.

o 평가방법 : 패치의 존재 여부와 존재하는 패치의 성격에 따라 Official Fix, Temporary Fix, Workaround, Unavailable로 구분한다. 해당 척도를 반영하지 않을 경우에는 Not Defined로 판정한다.

o 등급별 기준

등급	코드	점수	평가기준
Official Fix	OF	0.87	이용 가능한 완전한 벤더 솔루션이 있다. 취약점에 대하여 발표된 공식 패치를 가지고 있거나 취약점을 제거한 업그레이드 버젼이 이용 가능해야 한다.

Temporary Fix	TF	0.90	공식적인 임시 수정방법이 있다. 이는 벤더가 발표한 임시적인 응급 패치 프로그램, 툴, 임시방편을 포함한다.
Workaround	W	0.95	비공식적인 제 3자의 해결방법이 있다. 어떤 경우에는 사용자가 스스로 해결하는 방법을 강구하고나, 회피하는 방법을 사용하기도 한다.
Unvailable	C	1.0	이용 가능한 솔루션이 없거나, 그것을 적용하는 것이 불가능하다.
Not Defined	ND	1.0	해당 척도는 평가에 반영되지 않음.

6. 보고의 신뢰성

가. 보고의 신뢰성 (Reporting Confidence, RC)

o 개요 : 이 메트릭은 보안 취약점의 존재와 이로 야기되는 알려진 기술적 문제점에 대한 신뢰도를 평가하기 위하여 사용된다.

o 평가방법 : 해당 보안 취약점이 존재만이 알려져 있는지, 혹은 보안 취약점으로 인하여 영향을 받는 소프트웨어 벤더의 확인을 받았는지를 판단한다. 보안 취약점의 존재가 확실해 질수록 해당 보안 취약점을 제거해야할 필요성이 높아진다. 따라서 보안 취약점이 소프트웨어 벤더나 혹은 믿을만한 출처에서 확인을 받을수록 평가 기준의 점수가 높아진다.

o 등급별 기준

등급	코드	점수	평가기준
Unconfirmed	UC	0.5	하나의 출처에서만 보고서가 존재하거나 여러 개의 상충되는 보고서가 존재하여 보안 취약점에 대한

			신뢰도가 낮은 경우이다.
Uncorroborated	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다.
Confirmed	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우이다.
Not Defined	ND	0.0	이 값을 주면 취약성 점수에 영향을 주지 않는다.

제 2 절 국내 보안 취약점 사례에 대한 시범평가

이 절에서는 40개의 국내 보안 취약점 사례에 대한 CVSS 시범평가에 대해서 기술한다. 시범평가 대상이 되는 40개의 국내 보안 취약점은 표 3-1에 기술되어 있다. 표 3-1에 나열된 40개의 보안 취약점 각각에 대하여 각 평가항목 별 평가 결과를 계속해서 수록한다.

[표 3-1] 국내 보안 취약점 사례

	보안 취약점 이름
[12-011]	PHP 원격코드 실행 취약점
[12-014]	FTP 접속 프로그램 로컬 파일 실행 취약점
[12-016]	Cisco-NX-OS 서비스 거부 취약점
[12-019]	SSH 접속 프로그램 임의코드 실행 취약점
[12-023]	동영상 플레이어 버퍼 오버플로우 취약점
[12-029]	PHP-CGI 소스코드 노출
[12-034]	홈페이지 구축 소프트웨어 웹쉘코드 삽입 취약점
[12-052]	스마트폰 PC 연결 소프트웨어 원격코드 실행 취약점
[12-064]	워드프로세서 소프트웨어 임의코드 실행 취약점 #1
[12-071]	동영상 플레이어 DLL하이제킹 취약점

	보안 취약점 이름
[12-072]	워드프로세서 소프트웨어 임의코드 실행 취약점 #2
[12-075]	워드프로세서 소프트웨어 임의코드 실행 취약점 #3
[12-084]	에어컨 관리자 페이지 노출 취약점
[12-094]	동영상 플레이어 힙 오버플로우 취약점
[12-103]	NAS 관리자 페이지 계정정보 유출 취약점
[12-109]	홈페이지 구축 소프트웨어 XSS 취약점 #3
[12-129]	AcrobatReader X취약점
[12-131]	홈페이지 구축 소프트웨어 SQL Injection 취약점
[12-135]	메신저 프로그램 이미지 파일 공유 시 임의파일 업로드 취약점
[12-159]	Adobe Flash player 버퍼 오버플로우 취약점
[12-163]	그룹웨어 및 회계 관리 DB 시스템 관리자 계정 노출 취약점
[12-165]	결제 모듈 주요 개인정보 노출 취약점
[13-002]	홈페이지 구축 소프트웨어 XSS 취약점 #2
[13-005]	메신저 프로그램 계정 탈취 취약점
[13-020]	유무선 공유기 CSRF XSS 취약점
[13-021]	워드프로세서 소프트웨어 Integer Overflow 취약점 #1
[13-022]	백신 자체보호 기능 우회 취약점
[13-045]	워드프로세서 소프트웨어 스택 오버플로우
[13-050]	워드프로세서 소프트웨어 힙 오버플로우
[13-056]	메신저 프로그램 세션 노출 취약점
[13-057]	홈페이지 구축 소프트웨어 XSS 취약점 #3
[13-092]	홈페이지 구축 소프트웨어 원격 코드 실행
[13-105]	금융권 ActiveX 원격 코드 실행 취약점
[13-108]	워드프로세서 소프트웨어 Integer Overflow 취약점 #2
[13-109]	동영상 플레이어 원격코드 실행 취약점
[13-117]	압축 프로그램 Directory Traversal 취약점
[13-122]	워드프로세서 소프트웨어 Signed Extension Error Handling 취약점
[13-131]	웹에디터 소스코드 파일 다운로드 취약점
[13-162]	웹서버 프로그램 원격 코드 실행 취약점
[13-175]	DVR 장비 관리자 페이지 인증 우회 취약점

1. [12-011] PHP 원격코드 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	임의 코드 실행으로 인한 부분적으로 정보 기밀성에 영향을 줌.
무결성 영향 (I)	P	0.275	임의 코드 실행으로 인한 부분적으로 정보 무결성에 영향을 줌.
가용성 영향 (A)	P	0.275	임의 코드 실행으로 인한 부분적으로 시스템 가용성에 영향을 줌.
부수적 피해 잠재성(CDP)	LM	0.3	임의 코드 실행하는 서버로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	PHP 사용 환경이 매우 민감한 정보를 다루는 것은 아니므로 기밀성 요구가 특별히 크지는 않음.
무결성 요구 (IR)	H	1.51	PHP 사용 환경이 주로 서버이므로 정보 무결성 요구가 크다고 할 수 있음.
가용성 요구 (AR)	H	1.51	PHP 사용 환경이 주로 서버이므로 가용성 요구가 크다고 할 수 있음.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하므로 N으로 판정함
접근 복잡도 (AC)	L	0.71	특화된 접근조건이나 환경이 존재하지 않으며, 취약한 버전의 소프트웨어가 설치된 경우 공격이 가능하므로 L로 판정한다.
대응 난이도 (AR)	OF	0.87	공식적으로 제공된 패치 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	POC	0.9	공격의 개념을 시연할 수 있는 방법이 존재한다. 그러나, 특정 시스템에 대한 침해를 위해서는 해당 소프트웨어에 맞는 공격 방법을 사용해서 공격을 수행하여야 하므로 POC로 판정한다.
대상 분포 (TD)	H	1.0	PHP는 매우 광범위하게 사용되는 스크립트 언어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우이다. 벤더의 평가가 CVE 리스트에 등록되었으며, 패치가 개발되어 배포되었다.
중요도 전체 점수	7.8		

2. [12-014] FTP 접속 프로그램 로컬 파일 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	FTP 접속 프로그램 탐색창에서 로컬에 있는 파일의 실행과 관련한 취약점이므로 기밀성에 영향 없음.
무결성 영향 (I)	N	0	FTP 접속 프로그램 탐색창에서 로컬에 있는 파일의 실행과 관련한 취약점이므로 다른 시스템의 파일이나 정보의 변경을 하지 않는다.
가용성 영향 (A)	N	0	FTP 접속 프로그램 탐색창에서 로컬에 있는 파일의 실행과 관련한 취약점이므로 다른 시스템의 가용성에 대한 영향은 없다.
부수적 피해 잠재성(CDP)	L	0.1	FTP 접속 프로그램 탐색창에서 로컬에 있는 파일의 실행과 관련한 취약점이므로 피해 잠재성이 낮음.
기밀성 요구 (CR)	ND	1	기밀성 영향 없으므로 ND
무결성 요구 (IR)	ND	1	무결성 영향 없으므로 ND
가용성 요구 (AR)	ND	1	가용성 영향 없으므로 ND
접근 벡터 (AV)	N	1.0	공격과 관련한 접근 요구사항은 존재하지 않으므로 N으로 판정한다.
접근 복잡도 (AC)	H	0.35	특화된 실행상황이 필요하며, 이때 희생자가 존재하지 않는 파일을 수행하여야 하므로, 일반적인 적용이 힘듬
대응 난이도 (AR)	OF	0.87	공식적으로 제공된 패치 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	M	0.6	알FTP는 비교적 널리 사용되는 응용 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 26% - 75%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	0.6		

3. [12-016] Cisco-NX-OS 서비스 거부 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0.0	기밀성에 영향을 끼치지 않음.
무결성 영향 (I)	N	0.0	무결성에 영향을 끼치지 않음.
가용성 영향 (A)	C	0.660	스위치의 서비스가 거부됨으로써 이에 연결된 모든 네트워크 운용에 문제가 생길 수 있음.
부수적 피해 잠재성(CDP)	MH	0.4	스위치의 서비스가 거부됨으로써 이에 연결된 모든 네트워크 운용 문제로 중요한 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	ND	1	기밀성 영향 없으므로 ND
무결성 요구 (IR)	ND	1	무결성 영향 없으므로 ND
가용성 요구 (AR)	H	1.51	Cisco-NX-OS 사용환경은 가용성 요구가 높다고 볼 수 있음.
접근 벡터 (AV)	N	1.0	일반적인 원격 내트워크에서 공격 가능하므로 N으로 판정한다.
접근 복잡도 (AC)	L	0.71	특화된 접근조건이나 환경이 존재하지 않으며, 취약한 버전의 스위치 제품이 설치된 경우 공격이 가능하므로 L로 판정한다.
대응 난이도 (AR)	OF	0.87	공식적으로 제공된 패치 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 위험 패킷을 전송하는 방법으로 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	H	1.0	Cisco 스위치는 매우 광범위하게 사용되는 네트워크 장비로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우이다. 벤더의 평가가 CVE 리스트에 등록되었으며, 패치가 개발되어 배포되었다.
중요도 전체 점수	9.2		

4. [12-019] SSH 접속 프로그램 임의코드 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0.0	버퍼 오버플로우 발생이 가능성을 보였으나 공격 성공을 위한 조건이 어려워 기밀성에 영향은 거의 없음.
무결성 영향 (I)	N	0.0	버퍼 오버플로우 발생이 가능성을 보였으나 공격 성공을 위한 조건이 어려워 무결성에 영향은 거의 없음.
가용성 영향 (A)	P	0.275	버퍼 오버플로우 발생이 가능성을 보였으나 공격 성공을 위한 조건이 어려워 Xshell 클라이언트의 가용성에 부분적인 영향이 있을 수 있음.
부수적 피해 잠재성(CDP)	L	0.1	공격 성공을 위한 조건이 어려워, 최소한의 잠재적피해가 있을 수 있음.
기밀성 요구 (CR)	ND	1.0	기밀성 영향이 없으므로 ND
무결성 요구 (IR)	ND	1.0	무결성 영향이 없으므로 ND
가용성 요구 (AR)	MH	1.0	Xshell 사용 환경이 특별한 가용성 요구가 있다고 볼 수 없음.
접근 벡터 (AV)	N	1.0	일반적인 원격 내트워크에서 공격 가능하므로 N으로 판정한다.
접근 복잡도 (AC)	M	0.61	사용자가 해당 프로그램을 사용하여 위험한 서버에 접근하도록 사회공학적 방법을 사용해야하므로, M으로 판정한다.
대응 난이도 (AR)	OF	0.87	공식적으로 제공된 패치 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	POC	0.9	공격의 개념을 시연할 수 있는 방법이 존재한다. 그러나, 숙련된 공격자에 의한 과정을 필요로 하며 실제적인 침해를 위해서는 explit 코드를 작성해야 하므로 POC로 판정한다.
대상 분포 (TD)	L	0.3	SSH 접속 프로그램이 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우로 벤더에 의한 패치가 개발되어 배포되었다.
중요도 전체 점수	1.1		

5. [12-023] 동영상 플레이어 버퍼 오버플로우 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	버퍼 오버플로우 취약점이 보고되었지만 악성코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 기밀성에 영향은 거의 없을 것으로 판단됨.
무결성 영향 (I)	N	0	위와 같은 이유로 무결성에 영향은 거의 없을 것으로 판단됨.
가용성 영향 (A)	P	0.275	버퍼 오버플로우 취약점이 보고되었지만 악성코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 가용성에 부분적인 영향이 있을 수 있음.
부수적 피해 잠재성(CDP)	L	0.1	곰플레이어는 개인 PC 환경에서 사용되며 악성코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 그 피해 잠재성은 낮을 것으로 판단됨.
기밀성 요구 (CR)	ND	1.0	기밀성 영향 없으므로 ND
무결성 요구 (IR)	ND	1.0	무결성 영향 없으므로 ND
가용성 요구 (AR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 가용성에 대한 특별한 요구는 없다.
접근 벡터 (AV)	N	1.0	위험한 수행을 위하여 사회공학적 방법을 포함한 다양한 방법이 시도될 수 있으며, 이는 특별히 접근의 근접성과는 무관하다.
접근 복잡도 (AC)	H	0.35	사용자가 해당 프로그램을 사용하여 위험한 주소값을 접근하도록 사회공학적 방법을 사용해야 하나, 보안에 지식이 있는 사용자가 이러한 작업을 할 가능성이 매우 적으므로, High로 판정한다.
대응 난이도 (AR)	OF	0.87	공식적으로 제공된 패치 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	M	0.6	곰플레이어는 비교적 널리 사용되는 응용 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 26% - 75%이다.
보고의 신뢰성 (RC)	UC	0.5	하나의 출처에서만 보고서가 존재하거나 여러 상충되는 보고서가 존재하여 보안 취약점에 대한 신뢰도가 낮음.
중요도 전체 점수	1.1		

6. [12-029] PHP-CGI 소스코드 노출

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	서버 쪽 애플리케이션의 소스코드가 유출될 경우 웹 애플리케이션 로직의 전반 및 데이터베이스 정보 등이 노출될 수 있으나 이 취약점은 CGI 방식을 사용할 때만 적용되므로 그 영향은 부분적임.
무결성 영향 (I)	P	0.275	위와 같은 이유이나 이 취약점은 CGI 방식을 사용할 때만 적용되므로 그 영향은 부분적임.
가용성 영향 (A)	P	0.275	위와 같은 이유이나 이 취약점은 CGI 방식을 사용할 때만 적용되므로 그 영향은 부분적임.
부수적 피해 잠재성(CDP)	L	0.1	현재 PHP는 대부분 CGI 방식이 아닌 SAPI나 FastCGI 방식으로 구동되므로 해당 취약점의 피해 잠재성은 낮음.
기밀성 요구 (CR)	MH	1.0	PHP-CGI를 이용하는 환경이 특별한 기밀성 요구가 있다고 볼 수 없음.
무결성 요구 (IR)	MH	1.0	PHP-CGI를 이용하는 환경이 특별한 무결성 요구가 있다고 볼 수 없음.
가용성 요구 (AR)	MH	1.0	PHP-CGI를 이용하는 환경이 특별한 가용성 요구가 있다고 볼 수 없음.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	M	0.61	CGI 방식으로 PHP가 설치되어 있을 경우 쉽게 침해를 수행할 수 있으나 일반적인 설치 형태가 아니므로 M로 판정
대응 난이도 (AR)	OF	0.87	공식적으로 권장하는 방식으로 설치 방식을 바꾸면 문제점이 발생하지 않으므로, OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 취약한 형태로 설치된 대부분의 상황에서 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	L	0.3	PHP를 CGI 환경에서 사용하는 경우는 그리 많지 않기 때문에 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우이다. 벤더의 평가가 CVE 리스트에 등록되었으며, 패치가 개발되어 배포되었다.
중요도 전체 점수	1.7		

7. [12-034] 홈페이지 구축 소프트웨어 웹쉘코드 삽입 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	C	0.660	웹쉘 코드를 생성하여 원격 코드 실행이 가능함으로 정보 유출이 가능함.
무결성 영향 (I)	C	0.660	웹쉘 코드를 생성하여 원격 코드 실행이 가능하며 관리자 권한 탈취도 가능하여 데이터베이스 수정 및 조작이 가능함.
가용성 영향 (A)	C	0.660	웹쉘 코드를 이용한 공격은 서버에 대한 관리자 권한을 얻을 수 있기 때문에 해당 웹 서버를 이용 불가능하게 만들 수 있음.
부수적 피해 잠재성(CDP)	MH	0.4	웹쉘 코드 공격을 이용하여 정보를 유출 혹은 조작할 수 있으므로 중요한 물적 손실이 발생할 수 있으며 또한 해당 서버를 이용하여 내부망의 pc를 쉽게 공격할 수 있기 때문에 피해가 확산될 수 있음.현재 패치가 제공됨.
기밀성 요구 (CR)	MH	1.0	XE는 오픈소스 소프트웨어로 XE가 사용되는 사용자 환경은 기밀성에 대한 특별한 요구는 없다.
무결성 요구 (IR)	MH	1.0	XE는 오픈소스 소프트웨어로 XE가 사용되는 사용자 환경은 무결성에 대한 특별한 요구는 없다.
가용성 요구 (AR)	H	1.51	웹쉘은 주로 웹서버에서 사용되기 때문에 서버의 가용성이 중요하다고 할 수 있다.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	간단한 쉘코드 입력으로 쉽게 침해를 수행할 수 있으므로 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	L	0.3	XpressEngine은 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	2.2		

8. [12-052] 스마트폰 PC 연결 소프트웨어 원격코드 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	사용자의 PC에서 원격지의 악성코드가 실행되면 시스템 정보의 부분적으로 노출될 수 있음.
무결성 영향 (I)	P	0.275	사용자의 PC에서 원격지의 악성코드가 실행되면 시스템 정보의 무결성에 부분적인 영향이 있음.
가용성 영향 (A)	P	0.275	사용자의 PC에서 원격지의 악성코드가 실행되면 시스템의 가용성에 부분적인 영향이 있음.
부수적 피해 잠재성(CDP)	LM	0.3	사용자의 PC에서 원격지의 악성코드가 실행되면 시스템에 주는 영향으로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	삼성 kies소프트웨어를 사용하는 개인의 pc가 특별한 기밀성을 요구한다고 볼 수 없음.
무결성 요구 (IR)	MH	1.0	삼성 kies소프트웨어를 사용하는 개인의 pc가 특별한 무결성을 요구한다고 볼 수 없음.
가용성 요구 (AR)	MH	1.0	삼성 kies소프트웨어를 사용하는 개인의 pc가 특별한 가용성을 요구한다고 볼 수 없음.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	M	0.61	해당 소프트웨어의 침해를 위한 특화된 환경이 존재하지 않으나, 희생자가 위험한 사이트 접근하도록 하여야 하므로 M으로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	L	0.3	삼성 Kies 소프트웨어는 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.8		

9. [12-064] 워드프로세서 소프트웨어 임의코드 실행 취약점 #1

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	윈도우 XP 상에서 취약점이 존재하는 HWP 문서파일을 실행하면 악성파일이 자신의 컴퓨터에 설치되고 사용자의 개인정보를 지메일을 통해 외부로 유출을 시도하므로 기밀성에 부분적인 영향이 있음.
무결성 영향 (I)	N	0.0	정보 무결성에는 영향 없음.
가용성 영향 (A)	N	0.0	시스템 가용성에는 영향 없음.
부수적 피해 잠재성(CDP)	LM	0.3	정보부처의 정보들이 유출될 수 있으므로 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음,
기밀성 요구 (CR)	H	1.51	대량의 민감한 정보를 다루는 사용자가 있을 가능성이 높으므로 기밀성 요구가 높음.
무결성 요구 (IR)	ND	1.0	무결성 영향이 없으므로 ND
가용성 요구 (AR)	ND	1.0	가용성 영향이 없으므로 ND
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해 방법이 성공하므로 F로 판정한다.
대상 분포 (TD)	H	1.0	아래 한글은 매우 광범위하게 사용되는 워드 프로세스 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	5.2		

10. [12-071] 동영상 플레이어 DLL하이제킹 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	현재 디렉토리에 악성 DLL파일이 존재하는 경우에 실행될 수 있으나 악성 파일 삽입 메커니즘이 없으므로 기밀성 영향은 부분적이라고 판단됨.
무결성 영향 (I)	P	0.275	현재 디렉토리에 악성 DLL파일이 존재하는 경우에 실행될 수 있으나 악성 파일 삽입 메커니즘이 없으므로 무결성 영향은 부분적이라고 판단됨.
가용성 영향 (A)	P	0,275	현재 디렉토리에 악성 DLL파일이 존재하는 경우에 실행될 수 있으나 악성 파일 삽입 메커니즘이 없으므로 가용성 영향은 부분적이라고 판단됨.
부수적 피해 잠재성(CDP)	L	0.1	초코플레이어 사용자가 많지 않으며 악성파일 삽입 메커니즘이 없으므로 그 피해 잠재성은 낮다고 판단됨.
기밀성 요구 (CR)	MH	1.0	초코플레이어 사용자 환경이 특별한 기밀성 요구가 있다고 볼 수 없음.
무결성 요구 (IR)	MH	1.0	초코플레이어 사용자 환경이 특별한 무결성 요구가 있다고 볼 수 없음.
가용성 요구 (AR)	MH	1.0	초코플레이어 사용자 환경이 특별한 가용성 요구가 있다고 볼 수 없음.
접근 벡터 (AV)	N	1.0	위험한 파일의 업로드가 필요하며, 이는 접근 벡터와는 연관되지 않으므로 N으로 판정한다.
접근 복잡도 (AC)	H	0.35	실제적인 침해 전에 위험한 DLL의 업로드와 같은 사전 침해가 성공되어야 하므로 High로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 공격을 위한 DLL의 복사만으로 침해 방법이 대부분 성공하므로 F로 판정한다.
대상 분포 (TD)	L	0.3	초코플레이어 프로그램은 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.1		

11. [12-072] 워드프로세서 소프트웨어 임의코드 실행 취약점 #2

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	글상자 세부 정보 처리 시 힙 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성 영향은 부분적임.
무결성 영향 (I)	P	0.275	글상자 세부 정보 처리 시 힙 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 무결성 영향은 부분적임.
가용성 영향 (A)	P	0.275	글상자 세부 정보 처리 시 힙 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 가용성 영향은 부분적임.
부수적 피해 잠재성(CDP)	L	0.1	힙 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 약간의 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	한글 2010 이용 환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	한글 2010 이용 환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	한글 2010 이용 환경에 특별한 가용성 요구는 없음.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	악성 한글파일이 제시되었으며, 대부분 침해를 성공하므로 F로 판정한다.
대상 분포 (TD)	H	1.0	아래 한글은 매우 광범위하게 사용되는 워드 프로세스 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.6		

12. [12-075] 워드프로세서 소프트웨어 임의코드 실행 취약점 #3

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	공격자가 악성코드를 실행하여 정보의 기밀성에 부분적으로 영향을 줄 수 있음(사용자 PC 이름, IP 주소, 프록시 정보, 윈도우 운영체제 정보, 모듈경로 정보 등을 수집)
무결성 영향 (I)	P	0.275	공격자가 악성코드를 실행하여 정보의 무결성에 부분적으로 영향을 줄 수 있음.(특정 파일 업로드, 다운로드 및 C&C 서버 접속 등의 악의적인 행위)
가용성 영향 (A)	P	0.275	공격자가 악성코드를 실행하여 시스템의 가용성에 부분적으로 영향을 줄 수 있음.(특정 파일 업로드, 다운로드 및 C&C 서버 접속 등의 악의적인 행위)
부수적 피해 잠재성(CDP)	L	0.1	윈도우 XP에서 한글2005와 2007에서만 작동하며 이미 패치 조치되었으므로 그 피해는 미미함.
기밀성 요구 (CR)	H	1.51	정부부처를 대상으로 하므로 기밀성 요구가 높음.
무결성 요구 (IR)	H	1.51	정부부처를 대상으로 하므로 무결성 요구가 높음.
가용성 요구 (AR)	MH	1.0	가용성 요구가 특별히 높지는 않음.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	악성 한글파일이 제시되었으며, 대부분 침해를 성공하므로 F로 판정한다.
대상 분포 (TD)	H	1.0	아래 한글은 매우 광범위하게 사용되는 워드 프로세스 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	5.1		

13. [12-084] 에어컨 관리자 페이지 노출 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	냉난방시스템이 정보의 기밀성에 영향을 주지는 않음.
무결성 영향 (I)	N	0	냉난방시스템이 정보의 무결성에 영향을 주지는 않음.
가용성 영향 (AR)	C	0.660	악의적인 공격자가 공개된 ID와 PW를 이용하여 대상 대형 건물이나 병원 등의 냉난방 공조시스템을 완전히 사용 못하도록 차단하는 것이 가능함.
부수적 피해 잠재성(CDP)	LM	0.3	악의적인 공격자가 대형건물이나 병원 등의 냉난방 공조시스템을 완전히 사용 못하도록 차단하는 것이 가능하기 때문에 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	냉난방시스템과 관련된 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	냉난방시스템과 관련된 특별한 무결성 요구는 없음.
가용성 요구 (AR)	H	1.51	대형기업, 공공기업, 병원들의 냉난방시스템은 항상 사용 가능하여야하기 때문에 가용성에 대한 요구가 높다고 할 수 있음.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약한 시스템에 바로 접속 가능하므로 F로 판정한다.
대상 분포 (TD)	L	0.3	LG 에어컨 관리자 프로그램은 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	2.0		

14. [12-094] 동영상 플레이어 힙 오버플로우 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	곰플레이어의 힙 오버플로우 취약점이 보고되었지만 악성 코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 기밀성에 영향은 거의 없을 것으로 판단됨.
무결성 영향 (I)	N	0	곰플레이어의 힙 오버플로우 취약점이 보고되었지만 악성 코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 무결성에 영향은 거의 없을 것으로 판단됨.
가용성 영향 (A)	P	0.275	곰플레이어의 힙 오버플로우 취약점이 보고되었지만 악성 코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 가용성에 영향은 부분적일 것으로 판단됨.
부수적 피해 잠재성(CDP)	L	0.1	곰플레이어는 개인 PC 환경에서 사용되며 악성코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 그 피해 잠재성은 낮을 것으로 판단됨.
기밀성 요구 (CR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 기밀성에 대한 특별한 요구는 없다.
무결성 요구 (IR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 무결성에 대한 특별한 요구는 없다.
가용성 요구 (AR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 가용성에 대한 특별한 요구는 없다.
접근 벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	POC	0.9	공격의 개념을 시연할 수 있는 방법이 존재한다. 그러나, 숙련된 공격자에 의한 조절을 필요로 하므로 POC로 판정한다.
대상 분포 (TD)	M	0.6	곰플레이어는 비교적 널리 사용되는 응용 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 26% - 75%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	2.0		

15. [12-103] NAS 관리자 페이지 계정정보 유출 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	NAS 서버는 접속한 사용자들의 계정 관련 정보를 유출시킬 수 있음.
무결성 영향 (I)	N	0.0	NAS의 계정관련 정보가 유출되나 패스워드 평문을 확인하기 어려움으로 무결성에 영향 없음.
가용성 영향 (AR)	N	0.0	NAS의 계정관련 정보가 유출되나 패스워드 평문을 확인하기 어려움으로 시스템의 가용성에 대한 영향은 없음.
부수적 피해 잠재성(CDP)	L	0.1	NAS의 계정관련 정보가 유출되나 패스워드 평문을 확인하기 어려움으로 그 피해는 미미함.
기밀성 요구 (CR)	MH	1.0	기밀성 요구가 특별히 높지 않음.
무결성 요구 (IR)	ND	1	무결성 영향은 없으므로 ND
가용성 요구 (AR)	ND	1	시스템의 가용성에 대한 영향은 없으므로 ND
접근 벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	해당 취약점은 발견된 대부분의 상황에서 침해를 시연할 수 있는 방법이 제시되어 있으므로 F로 판정한다.
대상 분포 (TD)	L	0.3	LG NAS 프로그램은 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.1		

16. [12-109] 홈페이지 구축 소프트웨어 XSS 취약점 #3

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	게시글을 열람한 사용자의 PC에서 사용자정보를 탈취할 수 있으므로 정보 기밀성에 부분적인 영향을 줌.
무결성 영향 (I)	P	0.275	게시글을 열람한 사용자의 PC가 악성코드 전파, 피싱 등에 이용될 수 있으므로 정보 무결성에 부분적인 영향을 줌.
가용성 영향 (AR)	P	0.275	게시글을 열람한 사용자의 PC가 악성코드 전파, 피싱 등에 이용될 수 있으므로 시스템 가용성에 부분적인 영향을 줌.
부수적 피해 잠재성(CDP)	LM	0.3	기밀성과 무결성, 가용성 모두에 위협이 되는 공격이지만 그누보드의 특성상 부수적 피해 정도는 크지 않을 것으로 보임.
기밀성 요구 (CR)	MH	1.0	그누보드는 일반적으로 개인 홈페이지 등에 많이 이용되므로 기밀성이 크게 중요하지는 않음.
무결성 요구 (IR)	MH	1.0	그누보드는 일반적으로 개인 홈페이지 등에 많이 이용되므로 무결성이 크게 중요하지는 않음.
가용성 요구 (AR)	MH	1.0	그누보드는 일반적으로 개인 홈페이지 등에 많이 이용되므로 가용성이 크게 중요하지는 않음.
접근 벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	해당 취약점은 발견된 대부분의 상황에서 침해를 성공할 수 있는 방법이 제시되어 있으므로 F로 판정한다.
대상 분포 (TD)	L	0.3	그누보드4 프로그램은 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.8		

17. [12-129] Acrobat Reader X 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	Acrobat Reader X버전 에서는 프로그램 크래쉬 현상이 일어나는 POC 파일만 존재함으로 정보 기밀성에 영향은 없음.
무결성 영향 (I)	N	0	Acrobat Reader X버전 에서는 프로그램 크래쉬 현상이 일어나는 POC 파일만 존재함으로 정보 무결성에 영향은 없음.
가용성 영향 (AR)	N	0	Acrobat Reader X버전 에서는 프로그램 크래쉬 현상이 일어나는 POC 파일만 존재함으로 시스템 가용성에 영향은 없음.
부수적 피해 잠재성(CDP)	N	0	프로그램 크래쉬를 유발하는 POC 파일이 존재하나 임의코드 실행이 가능한 공격에 대한 내용은 없기 때문에 공격을 위해서는 추가 작업이 필요하며 만약 성공을 하여도 Acrobat Reader X의 보호기능의 우회가 어려워 피해 잠재성 거의 없음.
기밀성 요구 (CR)	ND	1	기밀성 영향이 없으므로 ND
무결성 요구 (IR)	ND	1	무결성 영향이 없으므로 ND
가용성 요구 (AR)	ND	1	가용성 영향이 없으므로 ND
접근 벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 정상적으로 처리하는 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	해당 취약점은 발견된 대부분의 상황에서 침해를 성공할 수 있는 방법이 제시되어 있으므로 F로 판정한다.
대상 분포 (TD)	N	0.0	해당 보안 취약점으로 인한 공격방법이 제시되지 않았기 때문에 침해가 예상되는 대상 시스템이 존재하지 않는다.
보고의 신뢰성 (RC)	UC	0.5	하나의 출처에서만 보고서가 존재하거나 여러 개의 상충되는 보고서가 존재하여 보안 취약점에 대한 신뢰도가 낮은 경우이다.
중요도 전체 점수	0.0		

18. [12-131] 홈페이지 구축 소프트웨어 SQL Injection 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	이 취약점의 SQL 인젝션을 통해 데이터베이스 정보 유출이 가능함으로 정보 기밀성에 부분적 영향이 있음.
무결성 영향 (I)	P	0.275	이 취약점의 SQL 인젝션을 통해 데이터베이스 정보 조작이 가능함으로 정보 무결성에 부분적 영향이 있음.
가용성 영향 (AR)	P	0.275	이 취약점의 SQL 인젝션을 통해 데이터베이스 정보 훼손이 가능함으로 시스템 가용성에 부분적 영향이 있음.
부수적 피해 잠재성(CDP)	LM	0.3	기밀성과 무결성, 가용성 모두에 위협이 되는 공격이지만 자유 소프트웨어인 그누보드의 특성상 상업용으로 많이 이용되지 않으므로 부수적 피해 정도는 크지 않을 것으로 보임.
기밀성 요구 (CR)	MH	1.0	자유 소프트웨어인 그누보드를 사용하는 환경은 기밀성 요구가 크지 않음.
무결성 요구 (IR)	MH	1.0	자유 소프트웨어인 그누보드를 사용하는 환경은 무결성이 요구가 크지 않음.
가용성 요구 (AR)	MH	1.0	자유 소프트웨어인 그누보드를 사용하는 환경은 가용성이 요구가 크지 않음.
접근 벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 정상적으로 처리하는 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	해당 취약점은 발견된 대부분의 상황에서 침해를 성공할 수 있는 방법이 제시되어 있으므로 F로 판정한다.
대상 분포 (TD)	L	0.3	그누보드 프로그램은 사용범위가 그리 넓지 않은 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 1% - 25%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.7		

19. [12-135] 메신저 프로그램 이미지 파일 공유 시 임의파일 업로드 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	각각 로그인한 사용자들 끼리 서로의 동의를 받아 이미지 파일을 공유하게 될 때에 악성파일을 상대방의 pc 아무 곳에 파일을 교체 혹은 저장이 가능함.
무결성 영향 (I)	P	0.275	이미지 파일을 공유하게 될 때에 악성파일을 상대방의 pc 아무 곳에나 저장하거나 기존 파일을 교체할 수 있으므로 무결성에 부분적인 영향이 있음.
가용성 영향 (A)	P	0.275	공격자는 악성 파일로 상대방의 주요 시스템 파일을 교체함으로써 시스템 가용성에 부분적인 영향을 미칠 수 있음.
부수적 피해 잠재성(CDP)	L	0.1	사진을 공유한 사람(한명 또는 여러명)에 한해 약간의 물적 손실의 결과를 낳을 수 있다.
기밀성 요구 (CR)	MH	1.0	네이트온 사용 환경이 특별히 무결성 요구가 높다고 할 수 없음.
무결성 요구 (IR)	MH	1.0	네이트온 사용 환경이 특별히 무결성 요구가 높다고 할 수 없음.
가용성 요구 (AR)	MH	1.0	네이트온 사용 환경이 특별히 가용성 요구가 높다고 할 수 없음.
접근 벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	M	0.61	네이트온을 사용하는 사용자에 대하여 공격이 가능하고 해당 사용자가 이미지를 공유하도록 유도하여야 하므로 M으로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	해당 취약점은 발견된 대부분의 상황에서 침해를 성공할 수 있으므로 F로 판정한다.
대상 분포 (TD)	H	1.0	네이트온 프로그램은 매우 광범위하게 사용되는 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.7		

20. [12-159] Adobe Flash player 버퍼 오버플로우 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	C	0.660	버퍼 오버플로우로 인해 악성코드 실행으로 정보가 공개될 수 있으며 이로 인해 모든 시스템 파일이 드러날 수 있다.
무결성 영향 (I)	C	0.660	버퍼 오버플로우로 인한 악성코드 실행으로 정보 무결성이 훼손될 수 있다.
가용성 영향 (A)	C	0.660	버퍼 오버플로우로 인한 악성코드 실행으로 시스템 자원이 완전히 사용 불가능할 수 있다.
부수적 피해 잠재성(CDP)	MH	0.4	시스템 훼손으로 인해 중요한 물적 손실이나 자산 손실의 결과를 낳을 수 있다.
기밀성 요구 (CR)	MH	1.0	Adobe Flash player 사용 환경에서 특별한 기밀성 요구는 없다.
무결성 요구 (IR)	MH	1.0	Adobe Flash player 사용 환경에서 특별한 무결성 요구는 없다.
가용성 요구 (AR)	MH	1.0	Adobe Flash player 사용 환경에서 특별한 가용성 요구는 없다.
접근 벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	악의적인 웹페이지를 통하여 수동적으로 공격이 수행되며, 부가적인 정보 수집 등이 필요 없으므로 Low로 판정한다.
대응 난이도 (AR)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	제시된 공격 파일을 통하여 취약한 소프트웨어 버전의 침해가 가능하므로 F
대상 분포 (TD)	H	1.0	Adobe Flash Player는 매우 광범위하게 사용되는 소프트웨어로 해당 보안 취약점으로 인하여 침해가 예상되는 대상 시스템들의 범위는 76% - 100%이다.
보고의 신뢰성 (RC)	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우이다. 벤더의 평가가 CVE 리스트에 등록되었으며, 패치가 개발되어 배포되었다.
중요도 전체 점수	9.2		

21. [12-163] 그룹웨어 및 회계 관리 DB 시스템 관리자 계정 노출 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	C	0.660	기업정보 및 회계정보로 유출로 중요한 기업 기밀이 유출될 수 있음.
무결성 영향 (I)	N	0	DB 관리자 계정 노출에 대한 언급은 있지만 구체적인 PoC는 없음
가용성 영향 (A)	N	0	DB 관리자 계정 노출에 대한 언급은 있지만 구체적인 PoC는 없음
부수적 피해 잠재성(CDP)	LM	0.3	기업정보 및 회계정보 유출로 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	이 소프트웨어 사용 환경이 특별한 기밀성 요구가 있는 것은 아님.
무결성 요구 (IR)	MH	1.0	이 소프트웨어 사용 환경이 특별한 무결성 요구가 있는 것은 아님.
가용성 요구 (AR)	MH	1.0	이 소프트웨어 사용 환경이 특별한 가용성 요구가 있는 것은 아님.
접근벡터 (AV)	N	1.0	네트워크를 통하여 DB 서버 공격이 가능하므로 N으로 판정한다.
접근 복잡도 (AC)	L	0.71	특화된 접근조건이나 환경이 존재하지 않으며, 취약한 버전의 소프트웨어가 설치된 경우 공격이 가능하므로 L로 판정한다.
대응 수준(RL)	W	0.95	공식적 패치는 알려지지 않았으나, 패스워드 변경 등을 통하여 취약성을 제거할 수 있다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해가 가능하다.
대상 분포 (TD)	L	0.3	더존 그룹웨어는 사용자가 많지 않은 제한적인 소프트웨어로 대상 분포를 Low로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.9		

22. [12-165] 결제 모듈 주요 개인정보 노출 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	결제자의 개인정보로 유출로 기밀성에 부분적인 영향을 줌.
무결성 영향 (I)	N	0	정보 무결성에는 영향이 없음.
가용성 영향 (A)	N	0	시스템 가용성 영향이 없음.
부수적 피해 잠재성(CDP)	L	0.1	결제자의 개인정보 유출로 인한 낮은 정도의 피해 잠재성이 있음.
기밀성 요구 (CR)	H	1.5	이 소프트웨어는 온라인 결제에 사용되므로 특별한 기밀성 요구가 있음.
무결성 요구 (IR)	MH	1.0	이 소프트웨어 사용 환경이 특별한 무결성 요구가 있는 것은 아님.
가용성 요구 (AR)	MH	1.0	이 소프트웨어 사용 환경이 특별한 가용성 요구가 있는 것은 아님.
접근벡터 (AV)	N	1.0	일반적인 원격 내트워크에서 공격 가능하므로 N으로 판정한다.
접근 복잡도 (AC)	L	0.71	특화된 접근조건이나 환경이 존재하지 않으며, 영수증 저장 주소 사이트에 항상 접근이 공격이 가능하므로 L로 판정한다.
대응 수준(RL)	TF	0.90	벤더가 일부 수정한 것으로 판단되나, 완전한 수정인지 여부는 불확실 하므로 TF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해가 가능하다.
대상 분포 (TD)	H	1.0	해당 취약점이 발견되는 소프트웨어는 가장 널리 사용되는 금융관련 소프트웨어에 해당되므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.2		

23. [13-002] 홈페이지 구축 소프트웨어 XSS 취약점 #2

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	사용자의 정보(쿠키, 세션) 탈취로 인해 정보 기밀성에 부분적으로 영향을 줌.
무결성 영향 (I)	N	0	정보 무결성에 직접적인 영향은 없음.
가용성 영향 (A)	N	0	시스템 가용성에 직접적인 영향은 없음.
부수적 피해 잠재성(CDP)	L	0.1	사용자 정보 탈취로 인해 낮은 수준의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	XE 사용 환경이 매우 민감한 정보를 다루는 것은 아니므로 기밀성 요구가 특별히 크지는 않음.
무결성 요구 (IR)	MH	1.0	XE 사용 환경이 정보 무결성 요구가 특별히 크지는 않음.
가용성 요구 (AR)	H	1.51	XE는 주로 웹서버에서 사용되기 때문에 서버의 가용성이 중요하다고 할 수 있다.
접근벡터 (AV)	N	1.0	일반적인 원격 내트워크에서 공격 가능하므로 N으로 판정한다.
접근 복잡도 (AC)	L	0.71	취약한 제로보드에 대한 특별한 접근 조건은 일반적으로 존재하지 않으므로 L로 판정한다.
대응 수준(RL)	OF	0.87	공식적으로 제공된 패치 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	취약 소프트웨어가 설치된 대부분의 상황에서 침해가 가능하다.
대상 분포 (TD)	M	0.6	제로보드는 비교적 알려진 공개 소프트웨어에 해당하나 사용자가 제한적이므로 대상 분포를 Medium으로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	2.2		

24. [13-005] 메신저 프로그램 계정 탈취 취약점

평가항목	평가결과		평가 근거
기밀성 영향(C)	P	0.275	본인인증을 우회하여 다른 사람의 NATE 계정을 탈취하여 정보 기밀성에 부분적으로 영향을 줌.
무결성 영향(I)	P	0.275	본인인증을 우회하여 다른 사람의 NATE 계정을 탈취하여 정보 무결성에 부분적으로 영향을 줌.
가용성 영향(A)	P	0.275	본인인증을 우회하여 다른 사람의 NATE 계정을 탈취하여 계정 소유자의 가용성에 영향을 줌.
부수적 피해 잠재성(CDP)	LM	0.3	다른 사람의 계정 탈취로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구(CR)	MH	1.0	사용 환경이 매우 민감한 정보를 다루는 것은 아니므로 기밀성 요구가 특별히 크지는 않음.
무결성 요구(IR)	MH	1.0	사용 환경이 정보 무결성 요구가 특별히 크지는 않음.
가용성 요구(AR)	MH	1.0	사용 환경이 가용성 요구가 특별히 크지는 않음.
접근벡터(AV)	N	1.0	일반적인 원격 내트워크에서 공격 가능하므로 N으로 판정한다.
접근 복잡도(AC)	M	0.61	공격을 수행하기 전에 id, 이름, 핸드폰 번호 등의 정보를 수집하여야 하므로 M으로 판정한다.
대응 수준(RL)	U	1.0	보고시점에서 공식적인 패치는 존재하지 않으므로 U로 판정한다.
공격 가능성(EX)	F	0.95	대부분의 상황에서 시연 가능하나, 웜등을 통해서 자동으로 수행하기는 어렵다.
대상 분포(TD)	M	0.6	NATE 웹페이지는 상당한 숫자의 사용자를 확보하고 있는 페이지로 대상 분포를 Medium으로 판정한다.
보고의 신뢰성(RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	3.7		

25. [13-020] 유무선 공유기 CSRF XSS 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0.0	기밀성에 영향을 끼치지 않음. (관리자 권한 탈취 PoC가 없음)
무결성 영향 (I)	N	0.0	무결성에 영향을 끼치지 않음. (관리자 권한 탈취 PoC가 없음)
가용성 영향 (A)	P	0.275	공유기 설정을 변경함으로써 가용성에 부분적으로 영향을 줄 수 있음.
부수적 피해 잠재성(CDP)	L	0.1	공유기 설정 변경으로 인해 낮은 수준의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	ND	1	기밀성 영향 없으므로 ND
무결성 요구 (IR)	ND	1	무결성 영향 없으므로 ND
가용성 요구 (AR)	H	1.51	ipTIME 사용환경은 가용성 요구가 높다고 볼 수 있음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특별한 조건이나 설정을 요구하지 않으므로 L로 판정한다.
대응 수준(RL)	W	0.95	보고시점에서 공식적인 패치는 존재하지 않으나 재 3자의 불완전한 회피 방법은 존재하므로 W로 판정한다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나, 웜등을 통해서 자동으로 수행하기는 어렵다.
대상 분포 (TD)	M	0.6	해당 보안 취약점을 포함하는 소프트웨어를 이용하는 유무선 공유기는 상당한 숫자의 사용자를 확보하고 있는 하드웨어로 대상 분포를 Medium으로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	2.7		

26. [13-021] 워드프로세서 소프트웨어 Integer Overflow 취약점 #1

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	그림 파일 파싱 모듈에서 정수 오버플로우가 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성 영향은 거의 없음.
무결성 영향 (I)	N	0	그림 파일 파싱 모듈에서 정수 오버플로우가 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 무결성 영향은 거의 없음.
가용성 영향 (A)	P	0.275	그림 파일 파싱 모듈에서 정수 오버플로우가 발생 가능하므로 부분적으로 가용성에 영향을 줌.
부수적 피해 잠재성(CDP)	L	0.1	정수 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	한글 2010 이용 환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	한글 2010 이용 환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	한글 2010 이용 환경에 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 파일을 전달하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	취약한 한글 파일 전달로 쉽게 침해를 수행할 수 있으므로 L로 판정한다.
대응 수준(RL)	U	1.0	이에 대한 제대로 작성된 공식적인 픽스는 없으며, 해당 보고는 최신 버전을 사용하고 있다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나, 웜등을 통해서 자동으로 수행하기는 어렵다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.0		

27. [13-022] 백신 자체보호 기능 우회 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	V3Lite 작동중지로 사용 PC가 악성코드에 노출됨에 따라 기밀성에 부분적인 영향이 있음.
무결성 영향 (I)	P	0.275	V3Lite 작동중지로 사용 PC가 악성코드에 노출됨에 따라 무결성에 부분적인 영향이 있음.
가용성 영향 (A)	P	0.275	V3Lite 작동중지로 사용 PC가 악성코드에 노출됨에 따라 가용성에 부분적인 영향이 있음.
부수적 피해 잠재성(CDP)	LM	0.3	V3Lite 작동중지로 사용 PC가 악성코드에 노출됨에 따라 어느 정도 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	V3Lite 사용환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	V3Lite 사용환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	V3Lite 사용환경에 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	해당 소프트웨어의 침해를 위한 특화된 환경이 존재하지 않으므로 L로 판정한다.
대응 수준(RL)	ND	1.0	관련 패치 존재 여부를 판단하기 어려우므로 해당 척도는 평가에 반영되지 않음.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파 여부는 경우에 따라 의존적이다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 V3 Lite 백신 프로그램은 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	6.5		

28. [13-045] 워드프로세서 소프트웨어 스택 오버플로우

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	악의적으로 조작된 파일을 열 경우 스택 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성 영향은 거의 없음.
무결성 영향 (I)	N	0	악의적으로 조작된 파일을 열 경우 스택 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 무결성 영향은 거의 없음.
가용성 영향 (A)	P	0.275	악의적으로 조작된 파일을 열 경우 스택 오버플로우 발생 가능하므로 부분적으로 가용성에 영향을 줌.
부수적 피해 잠재성(CDP)	L	0.1	스택 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	한글 2010 이용 환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	한글 2010 이용 환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	한글 2010 이용 환경에 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	U	1.0	취약한 소프트웨어가 최신버전이므로 수정한 공식 버전은 존재하지 않는다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.0		

29. [13-050] 워드프로세서 소프트웨어 힙 오버플로우

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	BMP 이미지 파일을 열 경우 힙 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성 영향은 거의 없음.
무결성 영향 (I)	N	0	BMP 이미지 파일을 열 경우 힙 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 무결성 영향은 거의 없음.
가용성 영향 (A)	P	0.275	BMP 이미지 파일을 열 경우 힙 오버플로우 발생 가능하므로 부분적으로 가용성에 영향을 줌.
부수적 피해 잠재성(CDP)	L	0.1	힙 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	한글 2007 이용 환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	한글 2007 이용 환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	한글 2007 이용 환경에 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	U	1.0	취약한 소프트웨어가 최신버전이므로 수정한 공식 버전은 존재하지 않는다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.0		

30. [13-056] 메신저 프로그램 세션 노출 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	카카오톡 세션 노출로 인한 대화도청, 전송으로 인해 부분적으로 정보 기밀성에 영향을 줌.
무결성 영향 (I)	N	0	카카오톡 세션 노출로 인한 정보 무결성에 영향은 거의 없음.
가용성 영향 (A)	N	0	카카오톡 세션 노출로 인한 가용성에 영향은 거의 없음.
부수적 피해 잠재성(CDP)	LM	0.3	카카오톡은 3천만 사용자를 갖고 있으므로 세션 노출만으로도 상당한 사회적 손실의 가능성이 있음.
기밀성 요구 (CR)	H	1.5	카카오톡 사용환경은 사적인 프라이버시 등의 기밀성 요구가 높음.
무결성 요구 (IR)	MH	1.0	카카오톡 사용환경은 정보 무결성 요구가 특별히 높지는 않음.
가용성 요구 (AR)	MH	1.0	카카오톡 사용환경은 가용성 요구가 특별히 높지는 않음.
접근벡터 (AV)	A	0.646	프록시 서버에 대한 접근이 제한될 수 있으므로, A로 판정한다.
접근 복잡도 (AC)	M	0.61	침해 전에 세션 정보의 수집 과정이 필요하므로 M으로 판정한다.
대응 수준(RL)	U	1.0	해당 취약점에 대한 수정 코드나 버전이 없으므로, U로 판정한다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 카카오톡 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.8		

31. [13-057] 홈페이지 구축 소프트웨어 XSS 취약점 #3

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	스크립트 실행으로 인해 부분적으로 정보 기밀성에 영향을 줌.
무결성 영향 (I)	P	0.275	스크립트 실행으로 인해 정보 무결성에 부분적으로 영향을 줄 수 있음.
가용성 영향 (A)	N	0	시스템 가용성에 직접적인 영향은 거의 없음.
부수적 피해 잠재성(CDP)	LM	0.3	스크립트 실행으로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	공개용 게시판 사용 환경이 매우 민감한 정보를 다루는 것은 아니므로 기밀성 요구가 특별히 크지는 않음.
무결성 요구 (IR)	MH	1.0	공개용 게시판 사용 환경이 정보 무결성 요구가 특별히 크지는 않음.
가용성 요구 (AR)	H	1.51	게시판은 주로 웹서버에서 사용되기 때문에 서버의 가용성이 중요하다고 할 수 있다.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	W	0.95	최신 버전의 약점으로 공식적인 패치는 존재하지 않으나, XSS에 대한 비공식적인 해결 방법을 적용할 수 있다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	M	0.6	해당 취약점을 가지고 있는 소프트웨어들은 비교적 알려진 공개 소프트웨어에 해당하나 사용자가 제한적이므로 대상 분포를 Medium으로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	3.5		

32. [13-092] 홈페이지 구축 소프트웨어 원격 코드 실행

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	원격 코드 실행으로 정보유출이 가능하나 권한 관리가 엄격하면 적용되지 않음.
무결성 영향 (I)	P	0.275	원격 코드 실행이 가능하며 관리자 권한 탈취도 가능하여 데이터베이스 수정 및 조작이 가능하나 권한 관리가 엄격하면 적용되지 않음.
가용성 영향 (A)	P	0.275	원격 코드를 이용한 공격은 서버에 대한 관리자 권한을 얻을 수 있기 때문에 해당 웹 서버를 이용 불가능하게 만들 수 있으나 권한 관리가 엄격하면 적용되지 않음.
부수적 피해 잠재성(CDP)	MH	0.4	원격 코드 공격을 이용하여 정보를 유출 혹은 조작할 수 있으므로 중요한 물적 손실이 발생할 수 있음.
기밀성 요구 (CR)	MH	1.0	XE는 오픈소스 소프트웨어로 XE가 사용되는 사용자 환경은 기밀성에 대한 특별한 요구는 없다.
무결성 요구 (IR)	MH	1.0	XE는 오픈소스 소프트웨어로 XE가 사용되는 사용자 환경은 무결성에 대한 특별한 요구는 없다.
가용성 요구 (AR)	H	1.51	XE는 주로 웹서버에서 사용되기 때문에 서버의 가용성이 중요하다고 할 수 있다.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	U	1.0	해당 취약점을 수정한 공식 버전의 존재 여부는 불확실하고, 해당 소프트웨어가 최신버전이므로 U로 판정한다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	M	0.6	제로보드는 비교적 알려진 공개 소프트웨어에 해당하나 사용자가 제한적이므로 대상 분포를 Medium으로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.3		

33. [13-105] 금융권 ActiveX 원격 코드 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	C	0.660	nProtect Netizen은 금융권, 공공기관, 전자결제 등 대다수의 대형 사이트에 공급된 온라인 보안 솔루션으로 악성 코드 실행으로 인한 기밀성 영향이 매우 큼.
무결성 영향 (I)	C	0.660	nProtect Netizen은 금융권, 공공기관, 전자결제 등 대다수의 대형 사이트에 공급된 온라인 보안 솔루션으로 악성 코드 실행으로 인한 무결성 영향이 매우 큼.
가용성 영향 (A)	C	0.660	nProtect Netizen은 금융권, 공공기관, 전자결제 등 대다수의 대형 사이트에 공급된 온라인 보안 솔루션으로 악성 코드 실행으로 인한 가용성 영향이 매우 큼.
부수적 피해 잠재성(CDP)	H	0.5	nProtect Netizen은 금융권, 공공기관, 전자결제 등 대다수의 대형 사이트에 공급된 온라인 보안 솔루션으로 원격 코드 공격으로 인해 사회적으로 높은 수준의 피해가 발생할 잠재성을 갖고 있음.
기밀성 요구 (CR)	H	1.5	nProtect Netizen이 사용되는 환경은 금융권, 공공기관 등으로 기밀성 요구가 높음.
무결성 요구 (IR)	MH	1.0	nProtect Netizen이 사용되는 환경은 금융권, 공공기관 등으로 무결성 요구가 높음.
가용성 요구 (AR)	MH	1.0	nProtect Netizen이 사용되는 환경은 금융권, 공공기관 등으로 보안성 요구가 높음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	U	1.0	최신버전에 존재하는 취약점으로 공식 패치는 존재하지 않는다.
공격 가능성 (EX)	F	0.95	대부분의 OS와 브라우져에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	H	1.0	해당 취약점이 발견되는 소프트웨어는 가장 널리 사용되는 보안 관련 소프트웨어에 해당되므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	8.4		

34. [13-108] 워드프로세서 소프트웨어 Integer Overflow 취약점 #2

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	Gif 이미지 파일 필터 모듈의 정수 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성 영향은 거의 없음.
무결성 영향 (I)	N	0	Gif 이미지 파일 필터 모듈의 정수 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 무결성 영향은 거의 없음.
가용성 영향 (A)	P	0.275	Gif 이미지 파일 필터 모듈의 정수 오버플로우 발생 가능하므로 가용성에 부분적으로 영향을 줌.
부수적 피해 잠재성(CDP)	L	0.1	정수 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 약간의 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	한글 2010 이용 환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	한글 2010 이용 환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	한글 2010 이용 환경에 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 파일을 전달하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	취약한 한글 파일 전달로 쉽게 침해를 수행할 수 있으므로 L로 판정한다.
대응 수준(RL)	U	1.0	이에 대한 제대로 작성된 공식적인 픽스는 없으며, 해당 보고는 최신 버전을 사용하고 있다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나, 웜등을 통해서 자동으로 수행하기는 어렵다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.0		

35. [13-109] 동영상 플레이어 원격코드 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	곰플레이어 원격 코드 실행 가능성이 보고된 수준으로 기밀성에 영향은 부분적일 것으로 판단됨.
무결성 영향 (I)	P	0.275	곰플레이어 원격 코드 실행 가능성이 보고된 수준으로 무결성에 영향은 부분적일 것으로 판단됨.
가용성 영향 (A)	P	0.275	곰플레이어 원격 코드 실행 가능성이 보고된 수준으로 가용성에 영향은 부분적일 것으로 판단됨.
부수적 피해 잠재성(CDP)	LM	0.3	곰플레이어 원격 코드 실행 가능성이 보고된 수준으로 중간 정도의 피해 잠재성을 갖고 있음.
기밀성 요구 (CR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 기밀성에 대한 특별한 요구는 없다.
무결성 요구 (IR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 무결성에 대한 특별한 요구는 없다.
가용성 요구 (AR)	MH	1.0	곰플레이어는 개인 PC 환경에서 사용되므로 가용성에 대한 특별한 요구는 없다.
접근벡터 (AV)	N	1.0	네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	U	1.0	최신 취약점으로 이에 대한 패치는 아직 존재하지 않는다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나, 웜등을 통해서 자동으로 수행하기는 어렵다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 곰플레이어 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UC	0.5	하나의 출처에서만 보고서가 존재하거나 여러 개의 상충되는 보고서가 존재하여 보안 취약점에 대한 신뢰도가 낮은 경우이다.
중요도 전체 점수	5.5		

36. [13-117] 압축 프로그램 Directory Traversal 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	기밀성 영향은 없음.
무결성 영향 (I)	P	0.275	주요 경로 접근을 통해 윈도우 시스템의 무결성에 부분적인 영향을 줄 수 있음.
가용성 영향 (A)	N	0	직접적인 가용성 영향은 없음..
부수적 피해 잠재성(CDP)	L	0.1	일부 경로에 대한 시스템 무결성에 영향을 줌으로써 낮은 정도의 피해 잠재성을 갖고 있음.
기밀성 요구 (CR)	MH	1.0	일반적인 PC 환경에서 사용되므로 기밀성에 대한 특별한 요구는 없다.
무결성 요구 (IR)	MH	1.0	일반적인 PC 환경에서 사용되므로 무결성에 대한 특별한 요구는 없다.
가용성 요구 (AR)	MH	1.0	일반적인 PC 환경에서 사용되므로 가용성에 대한 특별한 요구는 없다.
접근벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	OF	0.87	해당 취약점을 수정한 공식 버전이 존재하므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	L	0.3	반디집은 사용자가 많지 않은 제한적인 소프트웨어로 대상 분포를 Low로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	1.1		

37. [13-122] 워드프로세서 소프트웨어 Signed Extension Error Handling 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	N	0	Signed Extension Error Handling을 잘못하여 메모리 주소 값을 변경할 수 있지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성 영향은 거의 없음.
무결성 영향 (I)	N	0	메모리 주소 값을 변경할 수 있지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 무결성 영향은 거의 없음.
가용성 영향 (A)	P	0.275	메모리 주소 값을 변경할 수 있으므로 가용성에 부분적으로 영향을 줌.
부수적 피해 잠재성(CDP)	L	0.1	메모리 주소 값을 변경할 수 있지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.
기밀성 요구 (CR)	MH	1.0	한글 2010 이용 환경에 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	한글 2010 이용 환경에 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	한글 2010 이용 환경에 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	네트워크를 통하여 파일을 전달하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	취약한 한글 파일 전달로 쉽게 침해를 수행할 수 있으므로 L로 판정한다.
대응 수준(RL)	U	1.0	이에 대한 제대로 작성된 공식적인 픽스는 없으며, 해당 보고는 최신 버전을 사용하고 있다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나, 웜등을 통해서 자동으로 수행하기는 어렵다.
대상 분포 (TD)	H	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	4.0		

38. [13-131] 웹에디터 소스코드 파일 다운로드 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	C	0.660	서버 쪽 애플리케이션의 소스코드가 유출될 경우 웹 애플리케이션 로직의 전반 및 데이터베이스 정보 등이 노출될 수 있으므로 가용성이 심각한 영향이 있음.
무결성 영향 (I)	P	0.275	서버 쪽 애플리케이션의 소스코드가 유출될 경우 웹 애플리케이션 로직의 전반 및 데이터베이스 정보 등이 노출되므로 무결성에 부분적 영향이 있음.
가용성 영향 (A)	P	0.275	서버 쪽 애플리케이션의 소스코드가 유출될 경우 웹 애플리케이션 로직의 전반 및 데이터베이스 정보 등이 노출되므로 가용성에 부분적 영향이 있음.
부수적 피해 잠재성(CDP)	LM	0.3	소스 코드 정보를 유출 혹은 조작할 수 있으므로 중간 정도의 물적 손실이 발생할 가능성이 있음.
기밀성 요구 (CR)	MH	1.0	Namo Cross Editor를 이용하는 환경이 특별한 기밀성 요구가 있다고 볼 수 없음.
무결성 요구 (IR)	MH	1.0	Namo Cross Editor를 이용하는 환경이 특별한 무결성 요구가 있다고 볼 수 없음.
가용성 요구 (AR)	MH	1.0	Namo Cross Editor를 이용하는 환경이 특별한 가용성 요구가 있다고 볼 수 없음.
접근벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	U	1.0	해당 취약점을 수정한 공식 버전은 발표되지 않은 것으로 판단되므로 U으로 판정한다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	L	0.3	나모 크로스에디터는 사용자가 많지 않은 제한적인 소프트웨어로 대상 분포를 Low로 판정한다.
보고의 신뢰성 (RC)	UR	0.7	독립적인 보안 회사나 연구 단체들에서 발행한 비공식적인 다수의 보고서가 존재하는 경우이다. 보고서에 의한 공격이 재연 가능하다.
중요도 전체 점수	2.1		

39. [13-162] 웹서버 프로그램 원격 코드 실행 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	C	0.660	웹쉘 코드를 생성하여 원격 코드 실행이 가능함으로 정보 유출이 가능함.
무결성 영향 (I)	C	0.660	웹쉘 코드를 생성하여 원격 코드 실행이 가능하며 관리자 권한 탈취도 가능하여 데이터베이스 수정 및 조작이 가능함.
가용성 영향 (A)	C	0.660	웹쉘 코드를 이용한 공격은 서버에 대한 관리자 권한을 얻을 수 있기 때문에 해당 웹 서버를 이용 불가능하게 만들 수 있음.
부수적 피해 잠재성(CDP)	MH	0.4	웹쉘 코드 공격을 이용하여 정보를 유출 혹은 조작할 수 있으므로 중요한 물적 손실이 발생할 수 있으며 또한 해당 서버를 이용하여 내부망의 pc를 쉽게 공격할 수 있기 때문에 피해가 확산될 수 있음.현재 패치가 제공됨.
기밀성 요구 (CR)	MH	1.0	Apache Struts2 사용 환경은 기밀성에 대한 특별한 요구는 없음.
무결성 요구 (IR)	MH	1.0	Apache Struts2 사용 환경은 기밀성에 대한 특별한 요구는 없음.
가용성 요구 (AR)	H	1.51	Apache Struts2 는 웹서버에서 사용되기 때문에 서버의 가용성이 중요하다고 할 수 있다.
접근벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	특화된 접근 조건이나 환경이 존재하지 않으며, 일반적인 환경에서 공격 수행이 가능하므로 접근 복잡도는 L로 판정한다.
대응 수준(RL)	OF	0.87	해당 취약점을 수정한 공식 버전이 발표되어 있으므로 OF로 판정한다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	M	0.6	해당 보안 취약점이 발견되는 Struts2는 웹서비스 개발에 비교적 많이 사용되는 시스템 소프트웨어로 대상 분포는 Medium으로 판정한다.
보고의 신뢰성 (RC)	C	1.0	보안 취약점이 해당 소프트웨어 벤더나 저작권자에 의해서 확인된 경우이다. 벤더의 평가가 CVE 리스트에 등록된 상태이다.
중요도 전체 점수	5.4		

40. [13-175] DVR 장비 관리자 페이지 인증 우회 취약점

평가항목	평가결과		평가 근거
기밀성 영향 (C)	P	0.275	DVR 웹 뷰어에 패스워드를 해쉉하지 않고 텍스트로 저장하므로 패스워드 유출로 인한 DVR 파일의 유출이 가능함.
무결성 영향 (I)	P	0.275	DVR 웹 뷰어에 패스워드를 해쉉하지 않고 텍스트로 저장하므로 패스워드 유출로 인한 DVR 파일의 무결성 부분적으로 영향을 줄 수 있음.
가용성 영향 (AR)	P	0.275	DVR 웹 뷰어에 패스워드를 해쉉하지 않고 텍스트로 저장하므로 패스워드 유출로 인한 DVR 파일의 사용에 부분적으로 영향을 줄 수 있음.
부수적 피해 잠재성(CDP)	LM	0.3	DVR 내에 저장된 파일의 손상으로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기밀성 요구 (CR)	MH	1.0	DVR 시스템과 관련된 특별한 기밀성 요구는 없음.
무결성 요구 (IR)	MH	1.0	DVR 시스템과 관련된 특별한 무결성 요구는 없음.
가용성 요구 (AR)	MH	1.0	DVR 시스템과 관련된 특별한 가용성 요구는 없음.
접근벡터 (AV)	N	1.0	일반적인 네트워크를 통하여 공격이 가능하다.
접근 복잡도 (AC)	L	0.71	해당 페이지에 대한 접근을 통하여 공격이 수행되며, 부가적인 정보 수집등이 필요 없으므로 Low로 판정한다.
대응 수준(RL)	OF	0.87	해당 취약점에 패치의 존재 여부는 불확실하다. 해당 취약점은 아직 공식적으로 발표되지 않은 최신 취약점이므로 해당 패치는 아직 없을 것으로 판단된다.
공격 가능성 (EX)	F	0.95	대부분의 상황에서 시연 가능하나 자동적인 전파는 가변적이다.
대상 분포 (TD)	L	0.3	삼성 DVR 웹뷰어는 사용자가 많지 않은 제한적인 소프트웨어로 대상 분포를 Low로 판정한다.
보고의 신뢰성 (RC)	UC	0.5	하나의 출처에서만 보고서가 존재하거나 여러 개의 상충되는 보고서가 존재하여 보안 취약점에 대한 신뢰도가 낮은 경우이다.
중요도 전체 점수	1.6		

제 3 절 시범평가 결과

1. 평가 항목별 점수

[표 3-1]의 40개 취약점에 대한 평가항목별 평가 결과를 요약하면 [표 3-2]와 같다.

[표 3-2] 평가 항목별 점수

	AV	AC	AU	C	I	A	E	RL	RC	CDP	TD	CR	IR	AR
[12-011]	1.00	0.71	0.704	0.275	0.275	0.275	0.90	0.90	1.00	0.3	1.0	1.00	1.51	1.51
[12-014]	1.00	0.35	0.704	0.000	0.000	0.000	0.95	0.80	0.70	0.1	0.6	1.00	1.00	1.00
[12-016]	1.00	0.71	0.704	0.000	0.000	0.660	0.95	0.90	1.00	0.4	1.0	1.00	1.00	1.51
[12-019]	1.00	0.61	0.704	0.000	0.000	0.275	0.90	0.80	1.00	0.1	0.3	1.00	1.00	1.00
[12-023]	1.00	0.35	0.704	0.000	0.000	0.275	0.95	0.80	0.50	0.1	0.6	1.00	1.00	1.00
[12-029]	1.00	0.61	0.704	0.275	0.275	0.275	0.95	0.80	1.00	0.1	0.3	1.00	1.00	1.00
[12-034]	1.00	0.71	0.704	0.660	0.660	0.660	0.95	0.80	0.70	0.4	0.3	1.00	1.00	1.51
[12-052]	1.00	0.61	0.704	0.275	0.275	0.275	0.95	0.90	0.70	0.3	0.3	1.00	1.00	1.00
[12-064]	1.00	0.71	0.704	0.275	0.000	0.000	0.95	0.80	0.70	0.3	1.0	1.51	1.00	1.00
[12-071]	1.00	0.35	0.704	0.275	0.275	0.275	0.95	0.90	0.70	0.1	0.3	1.00	1.00	1.00
[12-072]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	0.80	0.70	0.1	1.0	1.00	1.00	1.00
[12-075]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	0.80	0.70	0.1	1.0	1.51	1.51	1.00
[12-084]	1.00	0.71	0.704	0.000	0.000	0.660	0.95	0.80	0.70	0.3	0.3	1.00	1.00	1.51
[12-094]	1.00	0.71	0.704	0.000	0.000	0.275	0.90	0.80	0.70	0.1	0.6	1.00	1.00	1.00
[12-103]	1.00	0.71	0.704	0.275	0.000	0.000	0.95	0.90	0.70	0.1	0.3	1.00	1.00	1.00
[12-109]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	0.90	0.70	0.3	0.3	1.00	1.00	1.00
[12-129]	1.00	0.71	0.704	0.000	0.000	0.000	0.95	0.80	0.50	0.0	0.0	1.00	1.00	1.00
[12-131]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	0.80	0.70	0.3	0.3	1.00	1.00	1.00
[12-135]	1.00	0.61	0.704	0.275	0.275	0.275	0.95	0.90	0.70	0.1	1.0	1.00	1.00	1.00
[12-159]	1.00	0.71	0.704	0.660	0.660	0.660	0.95	0.90	1.00	0.4	1.0	1.00	1.00	1.00
[12-163]	1.00	0.71	0.704	0.660	0.000	0.000	0.95	0.95	0.70	0.3	0.3	1.00	1.00	1.00
[12-165]	1.00	0.71	0.704	0.275	0.000	0.000	0.95	0.90	0.70	0.1	1.0	1.50	1.00	1.00
[13-002]	1.00	0.71	0.704	0.275	0.000	0.000	0.95	0.87	0.70	0.1	0.6	1.00	1.00	1.51
[13-005]	1.00	0.61	0.704	0.275	0.275	0.275	0.95	1.00	0.70	0.3	0.6	1.00	1.00	1.00
[13-020]	1.00	0.71	0.704	0.000	0.000	0.275	0.95	0.95	0.70	0.1	0.6	1.00	1.00	1.51
[13-021]	1.00	0.71	0.704	0.000	0.000	0.275	0.95	1.00	0.70	0.1	1.0	1.00	1.00	1.00

[13-022]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	1.00	0.70	0.3	1.0	1.00	1.00	1.00
[13-045]	1.00	0.71	0.704	0.000	0.000	0.275	0.95	1.00	0.70	0.1	1.0	1.00	1.00	1.00
[13-050]	1.00	0.71	0.704	0.000	0.000	0.275	0.95	1.00	0.70	0.1	1.0	1.00	1.00	1.00
[13-056]	0.646	0.61	0.704	0.275	0.000	0.000	0.95	1.00	0.70	0.3	1.0	1.50	1.00	1.00
[13-057]	1.00	0.71	0.704	0.275	0.275	0.000	0.95	0.95	0.70	0.3	0.6	1.00	1.00	1.51
[13-092]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	1.00	0.70	0.4	0.6	1.00	1.00	1.51
[13-105]	1.00	0.71	0.704	0.660	0.660	0.660	0.95	1.00	0.70	0.5	1.0	1.50	1.00	1.00
[13-108]	1.00	0.71	0.704	0.000	0.000	0.275	0.95	1.00	0.70	0.1	1.0	1.00	1.00	1.00
[13-109]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	1.00	0.50	0.3	1.0	1.00	1.00	1.00
[13-117]	1.00	0.71	0.704	0.000	0.275	0.000	0.95	0.87	0.70	0.1	0.3	1.00	1.00	1.00
[13-122]	1.00	0.71	0.704	0.000	0.000	0.275	0.95	1.00	0.70	0.1	1.0	1.00	1.00	1.00
[13-131]	1.00	0.71	0.704	0.660	0.275	0.275	0.95	1.00	0.70	0.3	0.3	1.00	1.00	1.00
[13-162]	1.00	0.71	0.704	0.660	0.660	0.660	0.95	0.87	1.00	0.4	0.6	1.00	1.00	1.51
[13-175]	1.00	0.71	0.704	0.275	0.275	0.275	0.95	0.87	0.50	0.3	0.3	1.00	1.00	1.00

[표 3-3] 평가 메트릭 그룹 요약

메트릭 그룹	벡터
기본	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
시간	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
환경	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

2. 취약점의 중요도 점수 계산

CVSS에서 취약점 평가를 위한 기본 메트릭 그룹, 시간 메트릭 그룹, 환경 메트릭 그룹에 속한 각 평가항목의 가능한 값들을 요약하면 표 3-3과 같다.

기본 메트릭, 시간 메트릭, 환경 메트릭의 점수를 계산하는 공식과 알고리즘은 다음과 같다. 기본 메트릭 점수는 CVSS의 근본이 되는 계산

공식으로 다음과 같이 계산된다.

```
BaseScore =
   round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20* AccessVector*AccessComplexity*Authentication
f(impact) = 0 if Impact=0, 1.176 otherwise

AccessVector = case AccessVector of
                              requires local access: 0.395
                              adjacent network accessible: 0.646
                              network accessible: 1.0
AccessComplexity = case AccessComplexity of
                              high: 0.35
                              medium: 0.61
                              low: 0.71
Authentication = case Authentication of
                    requires multiple instances authentication: 0.45
                    requires single instance of authentication: 0.56
                    requires no authentication: 0.704
ConfImpact = case ConfidentialityImpact of none: 0.0
                                           partial: 0.275
                                           complete: 0.660
IntegImpact = case IntegrityImpact of  none: 0.0
                                        partial: 0.275
                                        complete: 0.660
AvailImpact = case AvailabilityImpact of none: 0.0
                                       partial: 0.275
                                       complete: 0.660
```

시간 메트릭 점수는 앞서 계산된 기본 메트릭 점수를 사용하여 계산되며 1~10 까지의 값을 갖는다. 또한 시간 메트릭 점수는 기본 메트릭 점수보다 높을 수는 없으며 낮다 하더라도 기본 메트릭 점수의 33%보다는 커야한다. 시간 메트릭 점수를 계산하는 공식은 다음과 같다.

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability*
                RemediationLevel*ReportConfidence)

Exploitability = case Exploitability of unproven: 0.85
                                       proof-of-concept: 0.9
                                       functional: 0.95
                                       high: 1.00
                                       not defined: 1.00
RemediationLevel = case RemediationLevel of
                                       official-fix: 0.87
                                       temporary-fix: 0.90
                                       workaround: 0.95
                                       unavailable: 1.00
                                       not defined: 1.00
ReportConfidence = case ReportConfidence of
                                       unconfirmed: 0.90
                                       uncorroborated: 0.95
                                       confirmed: 1.00
                                       not defined: 1.00
```

환경 메트릭 점수는 앞서 계산된 시간 메트릭 점수를 사용하여 계산되며 1~10 까지의 값을 갖는다. 또한 환경 메트릭 점수는 시간 메트릭 점수보다 높을 수는 없다. 다음은 환경 메트릭 점수를 구하는 공식이다.

EnvironmentalScore =round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)
AdjustedTemporal = TemporalScore recomputed with the BaseScore's
Impact subequation replaced with the AdjustedImpact equation
AdjustedImpact =min(10, 10.41*(1-(1-ConfImpact*ConfReq)
*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq)))
CollateralDamagePotential = case CollateralDamagePotential of
none: 0
low: 0.1
low-medium: 0.3
medium-high: 0.4
high: 0.5
not defined: 0
TargetDistribution = case TargetDistribution of none: 0
low: 0.25
medium: 0.75
high: 1.00
not defined: 1.00
ConfReq = case ConfReq of low: 0.5
medium: 1.0
high: 1.51
not defined: 1.0
IntegReq = case IntegReq of low: 0.5
medium: 1.0
high: 1.51
not defined: 1.0
AvailReq = case AvailReq of low: 0.5
medium: 1.0
high: 1.51
not defined: 1.0

CVSS 메트릭 점수는 취약점의 심각성(혹은 중요도)을 계산하는 공식적인 계산 방식으로 사용되고 있다. 예를 들어 취약점에 관한 기업 표준으로 사용되는 CVE 같은 곳에서는 각 취약점에 대해 CVSS 메트릭을 함께 제공하고 있다.

각 취약점에 대한 평가 결과 점수(기본 점수:BaseScore, 시간 점수:TemporalScore, 환경 점수:EnvScore)는 표 3-4와 같다.

3. 평가 결과 분석

표 3-3의 국내 취약점에 대한 CVSS 시범평가 결과는 [표 3-4]와 같다. 이 평가 결과를 취약점의 중요도 최종점수인 환경 점수에 따라 내림차순으로 정렬한 결과는 [표 3-5]와 같다.

[표 3-4] 평가 결과 점수

	Impact	Exploitability	Base Score	Temporal Score	Adj Impact	Adj Base	Adj Temp	Env Score
[12-011]	6.4	10.0	7.5	6.1	7.8	8.4	6.8	7.8
[12-014]	0.0	4.9	0.0	0.0	0.0	0.0	0.0	0.6
[12-016]	6.9	10.0	7.8	6.7	10.0	10.0	8.6	9.2
[12-019]	2.9	8.6	4.3	3.1	2.9	4.3	3.1	1.1
[12-023]	2.9	4.9	2.6	1.0	2.9	2.6	1.0	1.1
[12-029]	6.4	8.6	6.8	5.2	6.4	6.8	5.2	1.7
[12-034]	10.0	10.0	10.0	5.3	10.0	10.0	5.3	2.2
[12-052]	6.4	8.6	6.8	4.1	6.4	6.8	4.1	1.8
[12-064]	2.9	10.0	5.0	2.7	4.3	6.0	3.2	5.2
[12-071]	6.4	4.9	5.1	3.1	6.4	5.1	3.1	1.1
[12-072]	6.4	10.0	7.5	4.0	6.4	7.5	4.0	4.6
[12-075]	6.4	10.0	7.5	4.0	7.8	8.4	4.5	5.1
[12-084]	6.9	10.0	7.8	4.1	10.0	10.0	5.3	2.0
[12-094]	2.9	10.0	5.0	2.5	2.9	5.0	2.5	2.0
[12-103]	2.9	10.0	5.0	3.0	2.9	5.0	3.0	1.1
[12-109]	6.4	10.0	7.5	4.5	6.4	7.5	4.5	1.8

	Impact	Exploit ability	Base Score	Temporal Score	Adj Impact	Adj Base	Adj Temp	Env Score
[12-129]	0.0	10.0	0.0	0.0	0.0	0.0	0.0	0.0
[12-131]	6.4	10.0	7.5	4.0	6.4	7.5	4.0	1.7
[12-135]	6.4	8.6	6.8	4.1	6.4	6.8	4.1	4.7
[12-159]	10.0	10.0	10.0	8.6	10.0	10.0	8.6	9.2
[12-163]	6.9	10.0	7.8	4.9	6.9	7.8	4.9	1.9
[12-165]	2.9	10.0	5.0	3.0	4.3	6.0	3.6	4.2
[13-002]	2.9	10.0	5.0	2.9	2.9	5.0	2.9	2.2
[13-005]	6.4	8.6	6.8	4.5	6.4	6.8	4.5	3.7
[13-020]	2.9	10.0	5.0	3.2	4.3	6.0	3.8	2.7
[13-021]	2.9	10.0	5.0	3.3	2.9	5.0	3.3	4.0
[13-022]	6.4	10.0	7.5	5.0	6.4	7.5	5.0	6.5
[13-045]	2.9	10.0	5.0	3.3	2.9	5.0	3.3	4.0
[13-050]	2.9	10.0	5.0	3.3	2.9	5.0	3.3	4.0
[13-056]	2.9	5.5	2.9	1.9	4.3	3.9	2.6	4.8
[13-057]	4.9	10.0	6.4	4.0	4.9	6.4	4.0	3.5
[13-092]	6.4	10.0	7.5	5.0	7.2	8.0	5.3	4.3
[13-105]	10.0	10.0	10.0	6.7	10.0	10.0	6.7	8.4
[13-108]	2.9	10.0	5.0	3.3	2.9	5.0	3.3	4.0
[13-109]	6.4	10.0	7.5	3.6	6.4	7.5	3.6	5.5
[13-117]	2.9	10.0	5.0	2.9	2.9	5.0	2.9	1.1
[13-122]	2.9	10.0	5.0	3.3	2.9	5.0	3.3	4.0
[13-131]	8,5	10.0	8.9	5.9	8,5	8.9	5.9	2.1
[13-162]	10.0	10.0	10.0	8.3	10.0	10.0	8.3	5.4
[13-175]	6.4	10.0	7.5	3.1	6.4	7.5	3.1	1.6

[표 3-5] 평가 결과 점수 : 내림차순정렬

	Impact	Exploit ability	Base Score	Temporal Score	Adj Impact	Adj Base	Adj Temp	Env Score
[12-016]	6.9	10	7.8	6.7	10	10	8.6	9.2
[12-159]	10	10	10	8.6	10	10	8.6	9.2
[13-105]	10	10	10	6.7	10	10	6.7	8.4
[12-011]	6.4	10	7.5	6.1	7.8	8.4	6.8	7.8
[13-022]	6.4	10	7.5	5	6.4	7.5	5	6.5
[13-109]	6.4	10	7.5	3.6	6.4	7.5	3.6	5.5
[13-162]	10	10	10	8.3	10	10	8.3	5.4

	Impact	Exploit ability	Base Score	Temporal Score	Adj Impact	Adj Base	Adj Temp	Env Score
[12-064]	2.9	10	5	2.7	4.3	6	3.2	5.2
[12-075]	6.4	10	7.5	4	7.8	8.4	4.5	5.1
[13-056]	2.9	5.5	2.9	1.9	4.3	3.9	2.6	4.8
[12-135]	6.4	8.6	6.8	4.1	6.4	6.8	4.1	4.7
[12-072]	6.4	10	7.5	4	6.4	7.5	4	4.6
[13-092]	6.4	10	7.5	5	7.2	8	5.3	4.3
[12-165]	2.9	10	5	3	4.3	6	3.6	4.2
[13-021]	2.9	10	5	3.3	2.9	5	3.3	4
[13-045]	2.9	10	5	3.3	2.9	5	3.3	4
[13-050]	2.9	10	5	3.3	2.9	5	3.3	4
[13-108]	2.9	10	5	3.3	2.9	5	3.3	4
[13-122]	2.9	10	5	3.3	2.9	5	3.3	4
[13-005]	6.4	8.6	6.8	4.5	6.4	6.8	4.5	3.7
[13-057]	4.9	10	6.4	4	4.9	6.4	4	3.5
[13-020]	2.9	10	5	3.2	4.3	6	3.8	2.7
[12-034]	10	10	10	5.3	10	10	5.3	2.2
[13-002]	2.9	10	5	2.9	2.9	5	2.9	2.2
[13-131]	8,5	10	8.9	5.9	8,5	8.9	5.9	2.1
[12-084]	6.9	10	7.8	4.1	10	10	5.3	2
[12-094]	2.9	10	5	2.5	2.9	5	2.5	2
[12-163]	6.9	10	7.8	4.9	6.9	7.8	4.9	1.9
[12-052]	6.4	8.6	6.8	4.1	6.4	6.8	4.1	1.8
[12-109]	6.4	10	7.5	4.5	6.4	7.5	4.5	1.8
[12-029]	6.4	8.6	6.8	5.2	6.4	6.8	5.2	1.7
[12-131]	6.4	10	7.5	4	6.4	7.5	4	1.7
[13-175]	6.4	10	7.5	3.1	6.4	7.5	3.1	1.6
[12-019]	2.9	8.6	4.3	3.1	2.9	4.3	3.1	1.1
[12-023]	2.9	4.9	2.6	1	2.9	2.6	1	1.1
[12-071]	6.4	4.9	5.1	3.1	6.4	5.1	3.1	1.1
[12-103]	2.9	10	5	3	2.9	5	3	1.1
[13-117]	2.9	10	5	2.9	2.9	5	2.9	1.1
[12-014]	0	4.9	0	0	0	0	0	0.6
[12-129]	0	10	0	0	0	0	0	0

이들 국내 취약점에 대한 CVSS 시범평가 결과 중에 몇 개의 특징적인 취약점에 대한 평가 결과를 보다 자세히 분석해보면 다음과 같다.

[12-016] Cisco-NX-OS 서비스 거부 취약점

C, I, A 값 중 가용성 영향인 A 값만 Complete(0.660)를 받았으며 이를 바탕으로 기본 점수로 7.8 점을 받았으며 시간 점수로 6.7 점을 받았다. 이 취약점은 Cisco-NX-OS가 국내 인터넷 환경에 많이 분포하고 있으며 그 부수적 피해 잠재성이 크다고 할 수 있다. 이러한 환경을 바탕으로 환경 점수로 9.2 점을 받았다.

[12-034] 홈페이지 구축 소프트웨어 웹쉘코드 삽입 취약점

이 취약점은 C, I, A 값 모두 Complete(0.660)를 받았으며 이를 바탕으로 기본 점수 10.0을 받았으며 시간 점수는 5.3을 받았다. 그러나 Xpress Engine이 게시판 에 사용되는 자유 소프트웨어로 다른 범용 소프트웨어처럼 많이 사용되고 있지는 않으며 상업적인 용도로 많이 사용되지 않기 때문에 부수적 피해 잠재성이 많지 않다. 이러한 이유로 환경 점수는 2.2점을 받았다.

[12-159] Adobe Flash Player의 버퍼 오버플로우 취약점

이 취약점은 C,I,A 값 모두 Complete(0.660)를 받았으며 이를 바탕으로 기본 점수 10.0을 받았으며 시간 점수는 8.6을 받았다. Adobe Flash Player가 국내 인터넷 환경에 많이 분포되어 대부분의 PC에서 사용되고 있으며 이로 인해 그 부수적 피해 잠재성이 크다고 할 수 있다. 이러한 사용자 환경을 바탕으로 환경 점수로 9.2 점을 받았다.

[13-105] 금융권 ActiveX 원격 코드 실행 취약점

nProtect Netizen은 금융권, 공공기관, 전자결제 등 대다수의 대형 사이트에 공급된 온라인 보안 솔루션으로 악성 코드 실행으로 인한 기밀성, 무결성, 보안성 영향이 매우 크므로 이 취약점은 C,I,A 값 모두 Complete(0.660)를 받았으며 이를 바탕으로 기본 점수 10.0을 받았으며 시간 점수는 6.7을 받았다. nProtect Netizen은 금융, 공공기관, 전자결제

를 사용하는 거의 모든 PC에서 가장 널리 사용되는 보안 관련 소프트웨어에 해당되므로 이러한 사용자 환경을 바탕으로 환경 점수를 계산하여 8.4 점을 받았다.

[13-050] 워드프로세서 소프트웨어 힙 오버플로우

한글 2007 소프트웨어에서 BMP 이미지 파일을 열 경우 힙 오버플로우 발생 가능하지만 악성 코드 유포/실행 메커니즘을 제시하지 않았으므로 그 기밀성, 무결성 영향은 거의 없음으로 판정했으며 이 소프트웨어의 가용성에는 부분적으로 영향을 줄 수 있으므로 Partial(0.275)으로 판정한다. 이를 바탕으로 기본 점수 5.0을 받았으며 시간 점수는 3.3을 받았다. 이 취약점은 힙 오버플로우가 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있으며 해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 대상 분포를 High로 판정한다. 이러한 사용자 환경을 바탕으로 환경 점수 4.0점을 받았다.

제 4 장 CWSS 시범평가

제 1 절 CWSS 평가 항목 및 평가 기준

본 시범평가에서는 CWSS 평가항목을 다음과 같은 6개의 범주로 재분류하였으며, 각 범주에 속한 CWSS 평가항목의 평가 방법과 평가 기준은 다음과 같다.

- 파급도
- 기술적 영향
- 시스템 중요도
- 공격 난이도
- 대응 난이도
- 보고의 신뢰성

1. 파급도

가. 출현빈도 (Prevalence, P)

o 개요 : 이 평가 기준은 해당 보안 취약점이 발견되는 빈도를 평가한다.

o 평가방법 : 해당 보안 취약점이 발견되는 대상 시스템의 보급 정도를 평가한다. 사용자가 많고 사용 빈도가 높을수록 높은 값을 가지며, 제한적 환경에서만 사용되는 경우에는 상대적으로 낮은 값을 가진다.

o 등급별 기준

등급	코드	점수	평가기준
Widespread	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
High	H	0.9	해당 보안 취약점이 널리 알려진 시스템 소프트웨어나 하드웨어에 임베디드된 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
Common	C	0.8	해당 보안 취약점이 널리 알려진 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
Limited	L	0.6	해당 보안 취약점이 사용자가 많지 않은 제한적인 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
Unknown	U	0.5	해당 보안 취약점이 발견되는 대상 시스템에 대한 구체적인 관련 자료가 없을 경우에 이 등급을 부여한다.

나. 배포 범위 (Deployment Scope, SC)

◦ 개요 : 해당 보안 취약점에 의하여 영향을 받는 소프트웨어의 범위를 평가한다.

◦ 평가방법 : 주어진 보안 취약점이 만약 모든 배포 가능한 버전에 존재하는지, 아니면 특정한 플랫폼이나 설정에서만 발생하는지를 평가한다. 보고된 취약점의 경우는 발생 가능한 소프트웨어와 설정 등에 관한 정보가 이미 존재하므로 Unknown이나 Not applicable, 혹은 Quantified 등급은 판정하지 않는다.

◦ 등급별 기준

등급	코드	점수	평가기준
All	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
Moderate	Mod	0.9	해당 보안 취약점이 대상 시스템이 일반적으로 인스톨되는 플랫폼이나 설정에 존재하는 경우이다.
Rare	Rare	0.5	해당 보안 취약점이 사용빈도가 낮은 플랫폼이나 설정에 존재하는 경우이다.
Potentially Reachable	Pot	0.1	해당 보안 취약점이 존재하기는 하나 보안 취약점 자체가 접근 불가능한 코드(dead code)에 존재하는 경우이다.
Default	D	0.7	해당 보안 취약점으로 인한 침해 가능성이 해당 소프트웨어가 설치된 시스템의 특성에 따라 다양할 경우에 중간 값을 부여한다.

2. 기술적 영향

가. 기술적 영향 (Technical Impact, TI)

o 개요 : 해당 보안 취약점을 이용한 공격으로 침해당했을 경우, 공격 성공으로 인한 기술적인 심각성을 평가한다.

o 평가 방법 : CWE의 약점에 대한 Common Consequences 항목에 기술되어 있는 8가지 Technical Impact 내용을 평가하여 각각에 대한 점수를 합산한 후, 이를 기준으로 등급을 부여한다. 이때 관련성

이란 해당 약점으로 인한 직접적인 결과를 의미하며, 간접적인 침해는 제외하는 것을 원칙으로 하나, 간접적인 침해의 사례가 많을 경우에는 이를 포함시킬 수 있다. 8가지 항목과 각 항목에 대하여 부여하는 점수는 다음과 같다.

Technical Impact 항목	전적인 침해	부분적인 침해	관련 없음
Modify data	2	1	0
Read data	2	1	0
DoS: unreliable execution	2	1	0
DoS: resource consumption	2	1	0
Execute unauthorized code or commands	4	2	0
Gain privileges / assume identity	2	1	0
Bypass protection mechanism	2	1	0
Hide activities	2	1	0

◦ 등급별 기준

등급	코드	점수	평가기준
Critical	C	1.0	6점 이상
High	H	0.9	4점~5점
Medium	M	0.6	2점~3점
Low	L	0.3	1점
None	N	0.0	0점
Default	D	0.6	Default 등급은 일반적으로 사용하지 않음.

3. 시스템 중요도

가. 비즈니스 영향(Business Impact, BI)

o 개요 : 이 메트릭은 취약점을 이용한 공격이 성공하였을 때 비즈니스 혹은 임무에 미치게 되는 잠재작인 영향을 나타낸다.

o 평가방법 : 약점을 이용한 공격으로 발생 가능한 비즈니스/임무의 운영에 대한 피해의 정도에 따라 아래 표와 같이 비즈니스 영향의 정도를 등급으로 정한다. 이 메트릭의 가능한 값들은 아래 표에 있으며 비즈니스 영향이 클수록 점수는 커진다.

o 등급별 기준

등급	코드	점수	평가기준
Critical	C	1.0	비즈니스/임무가 완전히 실패할 수 있다.
High	H	0.9	비즈니스/임무의 운용이 크게 영향 받을 수 있다.
Midium	M	0.8	비즈니스/임무의 운용이 크게 영향 받을 수 있으나 정상적인 운용에 대규모의 피해는 없다.
Low	L	0.7	비즈니스/임무에 최소한의 영향이 있다.
None	N	0.0	비즈니스/임무에 최소한의 영향이 없다.
Default	D	0.6	C, H, M, L, N의 중간 값
Not Applicable	NA	1.0	이 값은 비즈니스와 무관한 상황에 사용될 수 있음

4. 공격 난이도

가. 침해 가능성 (EX)

o 개요 : 보안 취약점을 가진 시스템에 대하여 필요한 공격에 필요한 권한과 접근 방법 및 인증을 가지고 있는 공격자가 성공적으로 해당 보안약점을 공격하여 시스템의 보안을 침해할 수 있을 가능성을 평가한다.

o 평가방법 : 취약점 보고서의 공격 예시를 반영하여, 공격의 성공 가능성을 판단한다. 시스템의 특성에 따라 다양하게 분포되어 있을 경우 Default 값을 부여한다. 단, 본 평가는 취약점 자체의 특성에만 기반하며, 취약점 설치의 특성, 인증, 접근권한, 사용자와의 상호작용 등의 특성은 무시한다. 단 위험한 프로그램의 설치와 같은 선행 공격이 필요할 경우에는 Medium으로 판정한다.

o 등급별 기준

등급	코드	점수	평가기준
High	H	1.0	공격자가 발견된 해당 취약점에 접근하여 공격할 경우 침해를 성공할 확률이 높은 경우를 말하며, 안정적인 공격방법을 쉽게 개발할 수 있는 경우이다.
Medium	M	0.6	공격자가 해당 취약점을 공격할 확률이 높으나, 성공 확률이 가변적인 경우를 말한다. 또한, 성공의 경우에도 일반적으로 여러 번의 공격을 시도하게 된다.
Low	L	0.2	일반적으로 공격 대상이 될 확률이 매우 낮은 보안약점으로서 공격의 성공 가능성도 제한적인 경우이다.
None	N	0	공격당하거나 해당 취약점으로 인한 보안 침해가 없을 경우로서 단순한 버그인 경우이다.
Default	D	0.6	해당 보안약점으로 인한 침해 가능성이 해당 소프트웨어가 설치된 시스템의 특성에 따라 다양할 경우에 중간값을 부여한다.

나. 접근 벡터 (Access Vector, AV)

o 개요 : 이 메트릭은 취약점을 이용하여 침해를 수행하는 통로와 관련된 평가 척도로서, 원격의 접근을 통하여 침해가 가능할수록 높은 점수가 부여된다.

o 평가방법 : 제시된 취약점의 공격방법 예시를 참고하여, 침해를 위하여 주로 사용되는 접근 방법을 판단한다. 복수의 방법이 가능할 경우에는 가장 점수가 높은 등급을 선택한다. 이미 발표된 취약점을 기준으로 하여 평가를 수행하므로, Unknown 등급은 제외한다.

o 등급별 기준

등급	코드	점수	평가기준
Internet	I	1.0	일반적인 인터넷을 통하여 취약점을 침해할 수 있다.
Intranet	R	0.8	방화벽 등으로 차단된 사업체의 인트라넷 내에 접근하여야 침해가 가능하다. 해당 인트라 넷은 내부 멤버들에게 일반적으로 접근이 가능하다.
Private	P	0.8	제한적으로 정의된 신뢰되는 그룹만이 접근할 수 있는 개별 네트워크에 접근하여야 침해가 가능하다.
Adjacent Network	A	0.7	네트워크에 물리적으로 연결된 인터페이스를 통하여 침해가 이루어 질 수 있다. 예를 들어, local IP 서브넷, 블루투스, IEEE 802.11, 지역 이더넷 세그먼트 등이다.
Local	L	0.5	쉘 계정과 같이 운영체제에 대하여 직접 명령어를 수행하는 접근이 필요하다.

등급	코드	점수	평가기준
Physical	P	0.2	시스템에 대하여 USB, 키보드, CD, 마우스 등을 사용한 직접적인 물리적 접근이 있어야 침해가 가능한 경우이다.
Default	D	0.75	평가할 수 없는 경우 미디언값을 부여한다.

다. 상호작용 정도 (Level of Interaction, IN)

o 개요 : 취약점을 공격하는데 필요한 피공격자의 협조적인 행동의 요구 수준을 평가한다.

o 평가방법 : 해당 취약점에 대한 보고서의 공격 방법 사례를 참조하거나, 정보가 존재할 경우 CAPEC의 공격 패턴 등을 참고하여 등급에 따라 평가한다. 시스템의 환경에 따라 여러 기준에 모두 해당하는 경우 해당 값들의 중간(median) 값을 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
Automated	Aut	1.0	희생자측의 협조적인 행동이 필요 없다.
Limited / Typical	Ltd	0.9	희생자의 일반적인 행동(이메일 열람, 웹페이지 접근)이 동반되어야 침해가 가능하다.
Moderate	Mod	0.8	희생자가 경고 메시지를 무시하는 것과 같은 어느 정도 위험할 수 있는 작업을 수행하여야 해당 보안약점에 대한 공격이 이루어진다.

등급	코드	점수	평가기준
Opportunistic	Opp	0.3	공격자가 직접적으로 희생자를 직접적으로 유도할 수 없으며, 희생자의 실수나 다른 사용자의 동작에 대하여 그 피해를 수동적으로 확대시킬 수만 있다.
High	High	0.1	희생자가 잘못된 행동을 하도록 희생자에 대한 직접적인 접근을 포함한 복잡한 사회적 작업을 수행하여야 한다.
No interaction	NI	0.0	희생자의 동작과 관련없이 침해 발생의 가능성이 없으며, 일종의 버그로서만 존재한다.

라. 권한 요구도 (Required Privilege, RP)

o 개요 : 공격자가 취약점에 대한 공격을 수행하기 위하여 필요한 접근 권한을 평가한다.

o 평가방법 : 제시된 취약점의 공격방법 예시를 참고하여, 침해를 위하여 필요한 권한을 판단한다. 사용자의 접근 권한과는 상관없는 취약한 프로그램의 사용 등으로 인한 문제는 D를 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	1.0	취약점을 가진 코드에 접근하기 위하여 아무 권한도 필요하지 않음 경우를 말한다. 일반적으로 공개되어 있는 웹 페이지를 위한 웹 응용프로그램에서 발생되는 보안 취약점이나 이메일 등을 통한 공격은 None으로 평가한다.

등급	코드	점수	평가기준
Guest	G	0.9	특정한 관리자의 허락을 요구하지 않고, 불특정 다수에게 허용되는 회원가입 등을 통하여 접근할 수 있는 프로그램 코드의 경우에 해당된다.
Regular User	RU	0.7	특별한 관리자 권한이 없는 정규 사용자 권한을 필요로 하는 경우를 말한다.
Partially Privileged User	P	0.6	전체적인 관리자 권한은 필요 없으나, 백업과 같은 부분적인 관리자 권한을 필요로 하는 경우를 말한다.
Administrator	A	0.1	해당 소프트웨어와 운영체제 전체에 대한 접근 권한을 가진 시스템 관리자 권한이 필요한 경우를 말한다.
Default	D	0.8	해당 취약점에 대한 공격이 시스템의 환경에 따라 다양한 권한을 요구하는 경우 Default 등급으로 하며, 점수는 Guest와 Regular User의 중간값을 부여한다.

5. 대응 난이도

가. 수정 난이도 (Remediation Effort, RE)

o 개요 : 취약점을 제거하는데 필요한 난이도를 판단한다.

o 평가방법 : 해당 취약점에 대한 보고서의 공격 방법 사례와 관련 취약점 방어 기술의 동향을 참고하여, 취약점 방어의 난이도를 아래 기준에 따라 평가한다. 보고된 취약점 자체를 기준으로 평가하고, 평가의 일관성을 유지하는 것을 고려하므로, Unknown, Not Applicable, Quantified 등급은 제외한다.

o 등급별 기준

등급	코드	점수	평가기준
Extensive	E	1.0	교정을 위하여 설계와 전체 시스템 구조의 수정과 같은 전체적인 수정이 필요하여, 상당한 작업과 시간이 필요하다.
Moderate	M	0.9	소스 파일의 복수개의 모듈 수정과 같은 중간 정도의 수정이 필요하며, 설계와 구조에 대한 수정은 필요 없다.
Limited	L	0.8	한 모듈 내의 적은 수의 라인의 코드에 대한 수정을 요구하며, 일정한 수준의 노력과 시간이 필요하다.
Default	D	0.9	소스코드의 미확보와 취약점 특성 등으로 인하여 필요한 난이도를 평가할 수 없을 경우 중간 값을 점수로 부여한다.

나. 외부 제어의 효과 (External Control Effectiveness, EC)

o 개요 : 소프트웨어 외부의 추가적인 시스템을 통하여 해당 취약점을 제어하는 방법의 효과를 평가한다. 예를 들어, 주소 공간 임의 배치 (Address Space Layout Randomization, ASLR)과 같은 기술이 버퍼 넘침의 위험도를 감소할 수는 있지만 제거하지는 못하는 경우를 들 수 있다.

o 평가방법 : 아래 등급별 기준에 따라 외부 제어의 효과를 평가한다. 제어의 효과가 높을수록 취약점의 심각성 점수는 낮게 평가된다. 보고된 취약점 자체를 기준으로 평가하고, 평가의 일관성을 유지하는 것을 고려하므로, Unknown, Not Applicable, Quantified 등급은 제

외한다. 이메일이나 첨부 파일에 대한 사전 검사 등은 일반적으로 적용되기 어려우므로 고려하지 않는다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	1.0	외부적으로 제어할 수 있는 방법이 없다.
Limited	L	0.9	간단한 방법이나, 부분적인 제한만이 가능하며, 초보적인 공격에 대해서만 방어가 가능하다.
Moderate	M	0.7	일반적으로 사용되는 방어 방법이 존재하나, 지식을 가진 공격자에 의하여 필요한 노력이 동반될 경우 침해될 수 있다.
Indirect	I	0.5	해당 침해를 전적으로 방어하지는 못하나, 공격의 피해를 줄이는 방법이 존재한다. 예를 들어 ASLR 방법은 잘못된 코드의 수행은 막을 수 있으나 프로그램의 중단되는 결과는 감수하여야 한다.
Best Available	B	0.3	적용 가능한 방어 방법이 존재하나, 숙련된 공격자가 다른 취약점을 함께 사용하여 공격할 경우 침해가 발생할 수 있는 가능성이 존재한다.
Complete	C	0.1	약점에 대하여 전적으로 효과적인 방법이 존재한다. 예를 들어 sandbox 방법을 통하여 파일 접근을 제어할 수 있다.
Default	D	0.6	취약점에 대하여 다양한 후보 대응방법이 존재하나 그 효과가 명확하지 않을 경우에 중간값을 부여한다.

6. 보고의 신뢰성

가. 발견의 신뢰도 (FC)

o 개요 : 보고된 보안 취약점의 신뢰도를 평가한다.

o 평가방법 : 보고된 보안 취약점이 취약점으로 의미가 있으며, 공격자가 실제로 이용할 수 있는 형태인지를 판단한다. Unknown이나 Not applicable, 혹은 Quantified 등급은 판정하지 않는다.

o 등급별 기준

등급	코드	점수	평가기준
Proven True	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
Proven Locally True	LT	0.8	해당 보안 취약점이 존재하나 공격자가 이에 접근할 수 있는지의 여부는 밝혀지지 않았거나 명확하지 않은 경우이다.
Proven False	F	0.0	보고 자체가 오류이거나 해당 보안 취약점을 공격에 이용할 수 있는 방법이 없는 경우이다.
Default	D	0.8	해당 보안 취약점으로 인한 침해 가능성이 명확하지 않거나 해당 소프트웨어가 설치된 시스템의 특성에 따라 다양할 경우에 중간 값을 부여한다.

제 2 절 국내 보안 취약점 사례에 대한 시범평가

이 절에서는 40개의 국내 보안 취약점 사례를 가지고 CWSS 방법론을 이용하여 시범 평가한 결과에 대하여 기술한다. 시범평가 대상이 되는 40개의 국내 보안 취약점은 [표 4-1] 에 기술되어 있다.

[표 4-1] 국내 보안 취약점 사례

	보안 취약점 이름
[12-011]	PHP 원격코드 실행 취약점
[12-014]	FTP 접속 프로그램 로컬 파일 실행 취약점
[12-016]	Cisco-NX-OS 서비스 거부 취약점
[12-019]	SSH 접속 프로그램 임의코드 실행 취약점
[12-023]	동영상 플레이어 버퍼 오버플로우 취약점
[12-029]	PHP-CGI 소스코드 노출
[12-034]	홈페이지 구축 소프트웨어 웹쉘코드 삽입 취약점
[12-052]	스마트폰 PC 연결 소프트웨어 원격코드 실행 취약점
[12-064]	워드프로세서 소프트웨어 임의코드 실행 취약점 #1
[12-071]	동영상 플레이어 DLL하이제킹 취약점
[12-072]	워드프로세서 소프트웨어 임의코드 실행 취약점 #2
[12-075]	워드프로세서 소프트웨어 임의코드 실행 취약점 #3
[12-084]	에어컨 관리자 페이지 노출 취약점
[12-094]	동영상 플레이어 힙 오버플로우 취약점
[12-103]	NAS 관리자 페이지 계정정보 유출 취약점
[12-109]	홈페이지 구축 소프트웨어 XSS 취약점 #3
[12-129]	AcrobatReader X취약점
[12-131]	홈페이지 구축 소프트웨어 SQL Injection 취약점
[12-135]	메신저 프로그램 이미지 파일 공유 시 임의파일 업로드 취약점
[12-159]	Adobe Flash player 버퍼 오버플로우 취약점
[12-163]	그룹웨어 및 회계 관리 DB 시스템 관리자 계정 노출 취약점
[12-165]	결제 모듈 주요 개인정보 노출 취약점
[13-002]	홈페이지 구축 소프트웨어 XSS 취약점 #2

	보안 취약점 이름
[13-005]	메신저 프로그램 계정 탈취 취약점
[13-020]	유무선 공유기 CSRF XSS 취약점
[13-021]	워드프로세서 소프트웨어 Integer Overflow 취약점 #1
[13-022]	백신 자체보호 기능 우회 취약점
[13-045]	워드프로세서 소프트웨어 스택 오버플로우
[13-050]	워드프로세서 소프트웨어 힙 오버플로우
[13-056]	메신저 프로그램 세션 노출 취약점
[13-057]	홈페이지 구축 소프트웨어 XSS 취약점 #3
[13-092]	홈페이지 구축 소프트웨어 원격 코드 실행
[13-105]	금융권 ActiveX 원격 코드 실행 취약점
[13-108]	워드프로세서 소프트웨어 Integer Overflow 취약점 #2
[13-109]	동영상 플레이어 원격코드 실행 취약점
[13-117]	압축 프로그램 Directory Traversal 취약점
[13-122]	워드프로세서 소프트웨어 Signed Extension Error Handling 취약점
[13-131]	웹에디터 소스코드 파일 다운로드 취약점
[13-162]	웹서버 프로그램 원격 코드 실행 취약점
[13-175]	DVR 장비 관리자 페이지 인증 우회 취약점

[표 4-1]에 제시된 40개의 보안 취약점에 대한 각 평가항목 별 평가 결과는 다음과 같다.

1. [12-011] PHP 원격코드 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되므로 경우 이 등급을 부여한다.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>적용 범위
(SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향
(BI)</td><td>M</td><td>0.8</td><td>임의 코드 실행하는 서버로 인해 비즈니스/임무의 운영이 중간 정도의 영향을 받을 수 있음.</td></tr>
<tr><td>기술적 영향
(TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성
(EX)</td><td>H</td><td>1.0</td><td>공격자가 발견된 해당 취약점에 접근하여 공격할 경우 침해를 성공할 확률이 높으며 안정적인 공격 방법이 알려져 있다.</td></tr>
<tr><td>상호작용 정도
(IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터
(AV)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도
(RP)</td><td>N</td><td>1.0</td><td>취약점을 가진 PHP 프로그램이 인터넷에서 접근 가능할 경우 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
복구 난이도 (RE)	D	0.9	현재 패치가 제공되었으나, 어느 수준의 수정이 이루어졌는지 불확실하므로 Default 값을 부여한다.
외부방어의 효율성 (EC)	L	0.9	해당 취약점에 대한 외부 제어 방법은 특별히 알려진 바가 없으나, 방화벽을 통하여 부분적인 방어가 가능할 것으로 판단된다. 따라서 Limited로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	77.33		

2. [12-014] FTP 접속 프로그램 로컬 파일 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	Mod	0.9	해당 보안 취약점이 대상 시스템이 일반적으로 인스톨되는 플랫폼이나 설정에 존재하는 경우이다. 해당 보안 취약점은 한글판에만 존재하고 영문판에는 존재하지 않는 것으로 보고되었음.
산업적 영향 (BI)	L	0.7	알FTP 탐색창에서 로컬에 있는 파일의 실행과 관련한 취약점이므로 그 피해는 미미함.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>L</td><td>0.2</td><td>공격을 위한 이전 작업이 많이 소요되며, 실제 사용자가 존재하지 않는 프로그램을 수행한다 하더라도 이에 해당하는 파일이 악성코드로 존재하여야 하므로 공격 가능성이 매우 낮은 것으로 판단된다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>D</td><td>0.75</td><td>악성코드를 사용자의 폴더에 가져다 놓는 과정은 특별히 정해진 바가 없으므로 Default로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Opp</td><td>0.3</td><td>존재하지 않는 실행파일을 수행하도록 하여야 하므로, 직접적인 희생자의 유도가 어려운 것으로 판정하여 Opp로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>D</td><td>0.8</td><td>공격 코드가 시스템에 이미 존재하여야 하나 특별히 접근 권한과는 무관하므로, Default로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>L</td><td>0.8</td><td>단순 코드 오류로 판단되므로, Limited로 판정한다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>None</td><td>1.0</td><td>내부의 불완전한 소프트웨어 사용에 의한 것이므로 외부 제어 방법은 특별히 없다.</td></tr>
</table>

평가항목	평가결과		평가 근거
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	53.57		

3. [12-016] Cisco NX-OS 서비스 거부

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	H	0.9	스위치의 서비스가 거부됨으로써 이에 연결된 모든 네트워크 사용이 불가하므로 비즈니스/임무의 운용이 크게 영향 받을 수 있음.
기술적 영향 (TI)	M	0.6	TI 항목 / 점수 Modify data (2/1/0) 0 Read data (2/1/0) 0 DoS: unreliable execution (2/1/0) 2 DoS: resource consumption (2/1/0) 0 Execute unauthorized code or commands (4/2/0) 0 Gain privileges / assume identity (2/1/0) 0 Bypass protection mechanism (2/1/0) 0 Hide activities (2/1/0) 0 합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N) 2
침해 가능성 (EX)	H	1.0	공격 패킷을 전송할 경우 시스템이 재부팅 되므로, 침해를 성공할 확률이 높으며 안정적인 공격 방법이 알려져 있는 것으로 판단하여 H로 판정한다.

평가항목	평가결과		평가 근거
상호작용 정도 (IN)	I	1.0	일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.
접근 벡터 (AV)	Aut	1.0	희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.
권한 요구도 (RP)	N	1.0	취약점을 가진 스위치 제품에 인터넷으로 접근 가능할 경우 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	D	0.9	현재 패치가 제공되었으나, 어느 수준의 수정이 이루어졌는지 불확실하므로 Default 값을 부여한다.
외부방어의 효율성 (EC)	N	1.0	네트워크 스위치의 문제에 의한 취약점으로서 취약한 버전 사용시 패치 외에는 외부 제어 방법은 특별히 없다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	79.38		

4. [12-019] SSH 접속 프로그램 임의코드 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	H	0.9	해당 보안 취약점이 널리 알려진 시스템 소프트웨어나 하드웨어-임베디드 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	패치 발표 및 공격 성공을 위한 조건이 어려워, 비즈니스/임무의 피해 잠재성은 낮을 것으로 판단됨.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>M</td><td>0.6</td><td>취약한 프로그램을 사용하는 희생자가 공격을 위한 서버에 접속하더라도, 텔넷 접속은 일반적으로 다양한 방법이 제공되므로 공격의 성공 가능성은 가변적이다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Opp</td><td>0.3</td><td>희생자가 해당 소프트웨어를 사용하여 공격자가 운영하는 위험한 서버에 접근하도록 하여야 하나, 공격자가 이러한 행동을 직접적으로 유도하는 것이 어려우므로 Opportunistic으로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>희생자의 시스템이 공격 서버에 인터넷으로 접근 가능할 경우 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>L</td><td>0.8</td><td>인식되지 않는 입력을 버리는 코드만 추가하면 되므로 L로 판정한다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>N</td><td>1.0</td><td>희생자가 외부의 공격 서버에 접근하는 것을 막을 수 있는 적절한 방법이 없으므로 N으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	63.16		

5. [12-023] 동영상 플레이어 버퍼 오버플로우 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	D	0.7	해당 보안 취약점의 해당 플랫폼이나 환경에 대한 설명이 명확하지 않아 중간 값을 부여한다.
산업적 영향 (BI)	L	0.7	곰플레이어는 개인 PC 환경에서 사용되며 악성코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 그 피해 잠재성은 낮을 것으로 판단됨.
기술적 영향 (TI)	H	0.9	TI 항목 / 점수 Modify data (2/1/0) 0 Read data (2/1/0) 0 DoS: unreliable execution (2/1/0) 0 DoS: resource consumption (2/1/0) 0 Execute unauthorized code or commands (4/2/0) 4 Gain privileges / assume identity (2/1/0) 0 Bypass protection mechanism (2/1/0) 0 Hide activities (2/1/0) 0 합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N) 4

평가항목	평가결과		평가 근거
침해 가능성 (EX)	H	1.0	희생자가 해당 프로그램을 사용하여 위험한 코드를 열도록 할 경우 대부분 공격이 성공하게 되므로 H로 판정한다.
상호작용 정도 (IN)	D	0.75	접근 방법과는 직접적인 연관이 없으므로, Default로 판정한다.
접근 벡터 (AV)	H	0.1	희생자가 해당 소프트웨어를 사용하여 위험한 주소를 열도록 하여야 하나, 해당 주소는 일반적인 주소가 아닌 공격코드이므로 이를 위해서는 복잡한 사회적 작업이 필요할 것으로 판단된다.
권한 요구도 (RP)	D	0.8	공격자의 침해 성공과 공격자의 권한 획득은 직접적인 관계는 없으므로 Default로 판정한다.
복구 난이도 (RE)	L	0.8	URL 입력에 대한 필터링 코드만 추가하면 되므로 L로 판정한다.
외부방어의 효율성 (EC)	N	1.0	희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	56.04		

6. [12-029] PHP-CGI 소스코드 노출

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	Rare	0.5	해당 보안 취약점이 사용빈도가 낮은 특정 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	현재 PHP는 대부분 CGI 방식이 아닌 SAPI나 FastCGI 방식으로 구동되어 해당 취약점이 적용되는 사이트는 미미하므로 비즈니스 영향은 낮음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행할 경우 성공 가능성이 매우 높으며 공격 방법도 간단함.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>희생자의 시스템이 공격 서버에 인터넷으로 접근 가능할 경우 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>L</td><td>0.8</td><td>소스코드의 수정보다는 시스템 설치 설정을 변경하면 되므로, 일정 수준의 노력만 소요되므로 L로 판정한다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>L</td><td>0.9</td><td>잘못 설치된 PHP 사이트에 대하여 방화벽 등을 통하여 외부 접근에 대한 부분적인 제어 방법이 존재하므로 L로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">65.32</td></tr>
</table>

7. [12-034] 홈페이지 구축 소프트웨어 웹쉘코드 삽입 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>C</td><td>0.8</td><td>해당 보안 취약점이 널리 알려진 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>H</td><td>0.9</td><td>웹 쉘 코드 공격을 이용하여 정보를 유출 혹은 조작할 수 있으므로 자산손실이 발생할 수 있다. 또한 해당 서버를 이용하여 내부망의 PC를 쉽게 공격할 수 있기 때문에 피해가 확산될 수 있다.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행할 경우 성공 가능성이 매우 높으며 공격 방법도 간단함.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	P	0.6	해당 XE 소프트웨어에 대한 관리자 권한이 필요하므로 Partially Privileged User
복구 난이도 (RE)	L	0.8	해당 입력부분에 필터링 코드만 추가하면 수정이 가능할 것으로 판단된다.
외부방어의 효율성 (EC)	L	0.9	응용프로그램 방화벽 등을 통하여 비정상적인 입력을 방지하는 방법이 존재하나, 외부 접근에 대한 부분적인 제어 방법이므로 L로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	72.33		

8. [12-052] 스마트폰 PC 연결 소프트웨어 원격코드 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	H	0.9	해당 보안 취약점이 널리 알려진 시스템 소프트웨어나 하드웨어-임베디드 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	사용자의 PC에서 원격지의 악성코드가 실행되면 시스템에 주는 영향으로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향
(TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성
(EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행하고, 희생자가 협조적인 동작을 할 경우 성공 가능성이 매우 높음.</td></tr>
<tr><td>상호작용 정도
(IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터
(AV)</td><td>L</td><td>0.9</td><td>희생자가 위험한 웹사이트를 접근하는 일반적인 행동을 수행하여야 하므로 L로 판정한다.</td></tr>
<tr><td>권한 요구도
(RP)</td><td>N</td><td>1.0</td><td>희생자의 시스템이 공격 서버에 인터넷으로 접근 가능할 경우 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>복구 난이도
(RE)</td><td>M</td><td>0.9</td><td>복수개의 모듈에 대한 수정이 필요한 것으로 판단되므로 M으로 판정한다.</td></tr>
<tr><td>외부방어의
효율성 (EC)</td><td>N</td><td>1.0</td><td>희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성
(FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">82.79</td></tr>
</table>

9. [12-064] 워드프로세서 소프트웨어 임의코드 실행 취약점 #1

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>정보부처에 따라 민감한 사안을 다룰 수 있으므로 그 임무의 운용이 크게 영향 받을 수 있으나 정상적인 운용에 대규모의 피해는 없음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행하고, 희생자가 협조적인 동작을 할 경우 성공 가능성이 매우 높음.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>M</td><td>0.8</td><td>희생자가 출처가 불분명한 한글 파일을 열어보는 위험한 행동을 수행해야 하므로 M으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	L	0.8	버퍼 넘침이 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.
외부방어의 효율성 (EC)	N	1.0	희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	82.02		

10. [12-071] 동영상 플레이어 DLL하이제킹 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	L	0.6	해당 보안 취약점이 사용자가 많지 않은 제한적인 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	초코플레이어 사용자가 많지 않으며 악성파일 삽입 메커니즘이 없으므로 그 비즈니스 영향은 낮다고 판단됨.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>M</td><td>0.6</td><td>위험한 dll 업로드 침해가 선행적으로 필요하므로 M으로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>D</td><td>0.75</td><td>사용자의 취약한 소프트웨어 사용에 의한 것이므로 평가가 적합하지 않아 Default를 부여한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>L</td><td>0.9</td><td>희생자가 취약한 프로그램을 사용하기만 하면 침해가 발생하므로 Limited로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>D</td><td>0.8</td><td>공격 코드가 시스템에 이미 존재하여야 하나 특별히 접근 권한과는 무관하므로, Default로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>M</td><td>0.9</td><td>DLL 참조 절차의 수정 시 관련 모듈의 수정이 필요할 것으로 판단되어, M으로 판정한다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>N</td><td>1.0</td><td>희생자의 정상적인 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">63.68</td></tr>
</table>

11. [12-072] 워드프로세서 소프트웨어 임의코드 실행 취약점 #2

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>힙 오버플로우 발생 가능하지만 악성 코드 유포 실행 메커니즘을 제시하지 않았으므로 비즈니스/임무의 운영이 최소한의 영향을 받을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행하고, 희생자가 협조적인 동작을 할 경우 성공 가능성이 매우 높음.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
접근 벡터 (AV)	M	0.8	희생자가 출처가 불분명한 한글 파일을 열어보는 위험한 행동을 수행해야 하므로 M으로 판정한다.
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	L	0.8	버퍼 넘침이 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.
외부방어의 효율성 (EC)	N	1.0	희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	77.41		

12. [12-075] 워드프로세서 소프트웨어 임의코드 실행 취약점 #3

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	윈도우 XP에서 한글2005와 2007에서만 작동하며 이미 패치 조치되었으므로 그 피해는 미미함.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향
(TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성
(EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행하고, 희생자가 협조적인 동작을 할 경우 성공 가능성이 매우 높음.</td></tr>
<tr><td>상호작용 정도
(IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터
(AV)</td><td>M</td><td>0.8</td><td>희생자가 출처가 불분명한 한글 파일을 열어보는 위험한 행동을 수행하여야 하므로 M으로 판정한다.</td></tr>
<tr><td>권한 요구도
(RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>복구 난이도
(RE)</td><td>L</td><td>0.8</td><td>wcscpy를 수행하는 버퍼 넘침 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.</td></tr>
<tr><td>외부방어의
효율성 (EC)</td><td>N</td><td>1.0</td><td>희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성
(FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">77.41</td></tr>
</table>

13. [12-084] 에어컨 관리자 페이지 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>L</td><td>0.6</td><td>해당 보안 취약점이 사용자가 많지 않은 제한적인 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>악의적인 공격자가 대형건물이나 병원 등의 냉난방 공조시스템을 완전히 사용 못하도록 차단하는 것이 가능하기 때문에 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>2</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>매뉴얼에 제시된 패스워드로 쉽게 접근하여 침해 가능하므로 H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>N</td><td>1.0</td><td>희생자의 협조적 행동은 필요 없다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	L	0.8	wcscpy를 수행하는 버퍼 넘침 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.
외부방어의 효율성 (EC)	N	1.0	희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	69.72		

14. [12-094] 동영상 플레이어 힙 오버플로우 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	곰플레이어는 개인 PC 환경에서 사용되며 악성코드 삽입 및 실행 메커니즘을 보이지는 않았으므로 비즈니스/임무에 최소한의 영향이 있다.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>곰플레이어를 사용하는 사용자가 위험한 웹사이트에 접속할 경우 침해가 발생할 확률이 높으므로, H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Ltd</td><td>0.9</td><td>인터넷 접속을 통해 침해가 발생하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>L</td><td>0.8</td><td>버퍼 넘침 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>N</td><td>1.0</td><td>희생자의 잘못된 접근에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">79.03</td></tr>
</table>

15. [12-103] NAS 관리자 페이지 계정정보 유출 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>L</td><td>0.6</td><td>해당 보안 취약점이 사용자가 많지 않은 제한적인 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>NAS 서비스에는 문제가 없으나 그 계정정보 유출로 인해 비즈니스/업무에 최소한의 영향이 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>2</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>곰플레이어를 사용하는 사용자가 위험한 웹사이트에 접속할 경우 침해가 발생할 확률이 높으므로, H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	D	0.9	현재 패치가 제공되었으나, 어느 수준의 수정이 이루어졌는지 불확실하므로 Default 값을 부여한다.
외부방어의 효율성 (EC)	N	1.0	해당 공격에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	65.94		

16. [12-109] 홈페이지 구축 소프트웨어 XSS 취약점 #3

평가항목	평가결과		평가 근거
출현 빈도 (P)	C	0.8	해당 보안 취약점이 널리 알려진 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	기밀성과 무결성, 가용성 모두에 위협이 되는 공격이지만 그누보드의 특성상 비즈니스 혹은 임무에 중간 정도 영향이 있을 것으로 판단됨.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 보드에 접속하는 사용자에 대한 침해가 발생할 확률이 높으므로, H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Ltd</td><td>0.9</td><td>일반적인 웹페이지 접근에 의하여 침해가 발생하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>G</td><td>0.9</td><td>일반적으로 회원가입 수준의 권한을 요구하므로 Guest로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>D</td><td>0.9</td><td>현재 패치가 제공되었으나, 어느 수준의 수정이 이루어졌는지 불확실하므로 Default 값을 부여한다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>I</td><td>0.5</td><td>해당 공격에 대한 ip 필터링, 방화벽 등의 제어 방법이 존재하나, 전적인 방어는 어려우므로 Indirect로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">39.86</td></tr>
</table>

17. [12-129] Acrobat Reader 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>N</td><td>0.0</td><td>Acrobat Reader X버전에서는 프로그램 크래쉬가 되는 현상이 일어나는 POC파일만 존재하고 임의 코드를 실행할 수 있는 시나리오 등은 없으므로 비즈니스에 영향은 거의 없음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>L</td><td>0.3</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>1</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>Low</td><td>0.2</td><td>협조자가 웹 등을 통하여 전단된 취약한 파일을 열 경우 침해가 발생하나 침해의 종류가 프로그램의 종료이고, 추가적인 침해의 가능성은 매우 낮으므로 Low로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>M</td><td>0.8</td><td>희생자가 출처가 불분명한 pdf 파일을 열어보는 위험한 행동을 수행해야 하므로 M으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	L	0.8	버퍼 넘침 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.
외부방어의 효율성 (EC)	N	1.0	희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	F	0.0	해당 보안 취약점을 공격에 이용할 수 있는 방법이 현재까지는 보고되지 않은 경우이다.
중요도 점수	0.00		

18. [12-131] 홈페이지 구축 소프트웨어 SQL Injection 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	C	0.8	해당 보안 취약점이 널리 알려진 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	Rare	0.5	해당 보안 취약점이 사용빈도가 낮은 특정 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	기밀성과 무결성, 가용성 모두에 위협이 되는 공격이지만 자유 소프트웨어인 그누보드의 특성상 상업용으로 많이 이용되지 않으므로 비즈니스 혹은 임무에 영향은 낮을 것임.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>침해가 발생할 확률이 높으며, 간단한 공격 방법이 제시되어 있으므로, H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>Aut</td><td>1.0</td><td>희생자의 동작은 필요하지 않으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>L</td><td>0.8</td><td>SQL 삽입 취약점의 제거는 해당 부분의 부분적인 수정만으로 가능하므로 Limited로 판정한다.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>L</td><td>0.7</td><td>해당 공격에 대한 방화벽 등의 제어 방법이 존재하나 부분적인 방어만 가능하므로 Limited로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">48.99</td></tr>
</table>

19. [12-135] 메신저 프로그램 이미지 파일 공유 시 임의파일 업로드 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>All</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>사진을 공유한 사람(한명 또는 여러 명)에 한해 약간의 물적 손실의 결과를 낳을 수 있다.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>침해가 발생할 확률이 높으며, 간단한 공격 방법이 제시되어 있으므로, H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>M</td><td>0.8</td><td>희생자가 출처가 불분명한 이미지 파일을 저장하는 위험한 행동을 수행하여야 하므로 M으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
복구 난이도 (RE)	D	0.9	해당 취약점 제거를 위한 수정 범위가 불확실하므로 Default로 판정함.
외부방어의 효율성 (EC)	N	1.0	악의적인 플래시 파일 접근을 제한하는 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	77.88		

20. [12-159] Adobe Flash Player 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점이 가장 널리 사용되는 시스템 소프트웨어나 응용 소프트웨어에서 발견되는 경우 이 등급을 부여한다.
적용 범위 (SC)	All	1.0	해당 보안 취약점이 대상 시스템이 인스틀 되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	H	0.9	버퍼 오버플로우 공격이 이루어졌을 때 공격자는 완전히 해당 시스템을 장악하여 모든 파일정보와 자료를 변경, 삭제할 수 있으므로 비즈니스/임무가 크게 영향 받을 수 있다.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N)</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점이 알려져 있으며, 취약한 소프트웨어를 사용할 경우 침해가 발생할 확률이 높으므로, H로 판정한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>L</td><td>0.9</td><td>희생자가 플레시 등을 사용하는 웹페이지 접근시 침해를 당할 수 있으므로, Low로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>G</td><td>0.9</td><td>일반적인 회원가입 수준의 권한을 요구하므로 Guest로 판정한다.</td></tr>
<tr><td>복구 난이도 (RE)</td><td>D</td><td>0.9</td><td>해당 취약점 제거를 위한 수정범위가 불확실하므로 Default로 판정함.</td></tr>
<tr><td>외부방어의 효율성 (EC)</td><td>N</td><td>1.0</td><td>네이트를 통한 그림 고유를 제한하기 위한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">87.09</td></tr>
</table>

21. [12-163] 그룹웨어 및 회계 관리 DB 시스템 관리자 계정 노출 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>L</td><td>0.6</td><td>해당 그룹웨어는 사용자가 많지 않은 제한적인 소프트웨어에 해당하므로 Limited로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>기업정보 및 회계정보 유출로 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>2</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>접속 가능 DB 서버 정보를 알고 있으면, 대부분 접속이 가능하며, 자동화 툴을 사용하여 쉽게 스캔 가능하므로, 공격을 쉽게 성공할 수 있음.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>DB 서버를 인터넷을 통하여 쉽게 접근하여 침해할 수 있다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Aut</td><td>1.0</td><td>서버측의 협조적인 행동이 필요 없다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>취약점을 가진 DB 서버에 접근하기 위하여 일반적으로 특정 권한이 필요하지 않다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	M	0.9	고정된 패스워드 사용을 수정하여야 하므로, 복수개의 모듈 수정과 같은 중간 정도의 수정이 필요하며, 설계와 구조에 대한 수정은 필요없다.
외부 제어의 효과 (EC)	N	1.0	특별히 이 취약점을 위한 외부 제어 방법은 없다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	70.14		

22. [12-165] 결제 모듈 주요 개인정보 노출 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 취약점이 발견되는 소프트웨어가 가장 널리 사용되는 결제관련 소프트웨어에 해당되므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	결제자의 개인정보 유출로 인한 낮은 정도의 피해 잠재성이 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>2</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 URL을 사용하여 거래를 접근 가능하므로 성공 가능성이 높은 것으로 판단하여 H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>해당 URL로 접근만 하면 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>D</td><td>0.9</td><td>현재 일부 수정이 이루어진 것으로 판단되나, 어느 수준의 수정이 이루어졌는지 불확실하므로 Default 값을 부여한다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>네트워크 스위치의 문제에 의한 취약점으로서 취약한 버전 사용시 패치 외에는 외부 제어 방법은 특별히 없다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">70.98</td></tr>
</table>

23. [13-002] 홈페이지 구축 소프트웨어 XSS 취약점 #2

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>C</td><td>0.8</td><td>제로보드는 널리 알려진 응용 소프트웨어에 해당하므로 Common으로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>사용자 정보 탈취로 인해 낮은 수준의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>2</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>2</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 취약한 사이트에 위험한 스크립트를 업로드 하는 것이 어렵지 않고 성공 가능성이 높은 것으로 판단하여 H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Ltd</td><td>0.9</td><td>게시물에 접근하는 일반적인 동작이 필요하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>G</td><td>0.9</td><td>스크립트 업로드를 위한 회원 가입이 필요하다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	L	0.8	필터링 관련 코드만 수정하면 된다.
외부 제어의 효과 (EC)	M	0.7	XSS에 대한 일반적인 방어방법이 존재하나, 지식을 가진 공격자의 노력에 의해서 침해가 발생할 수 있다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	52.80		

24. [13-005] 메신저 프로그램 계정 탈취 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 웹서비스는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	다른 사람의 계정 탈취로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.
기술적 영향 (TI)	H	0.9	TI 항목 / 점수 Modify data (2/1/0) / 0 Read data (2/1/0) / 0 DoS: unreliable execution (2/1/0) / 0 DoS: resource consumption (2/1/0) / 0 Execute unauthorized code or commands (4/2/0) / 0 Gain privileges / assume identity (2/1/0) / 2 Bypass protection mechanism (2/1/0) / 2 Hide activities (2/1/0) / 0 합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N / 4

평가항목	평가결과		평가 근거
침해 가능성 (EX)	H	1.0	희생자가 관련 id, 핸드폰번호, 이름 정보를 알고 있을 경우 쉽게 침해에 성공할 수 있으므로 H로 판정한다.
접근 벡터 (AV)	I	1.0	일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.
상호작용 정도 (IN)	Aut	1.0	희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.
권한 요구도 (RP)	N	1.0	관련 정보만 알고 있으면 패스워드 탈취를 위한 회원가입은 불필요하다.
수정 난이도 (RE)	M	0.9	핸드폰을 사용한 인증과 관련된 코드 부분을 수정하여야 하므로, 복수개의 모듈에 대한 중간 정도의 수정이 필요하다.
외부 제어의 효과 (EC)	N	1.0	해당 취약성을 위한 특정 외부 제어 방법은 없다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	85.92		

25. [13-020] 유무선 공유기 CSRF XSS 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	H	0.9	해당 보안 취약점은 널리 사용되는 하드웨어의 시스템 소프트웨어이므로 High로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	공유기 설정 변경으로 인해 낮은 수준의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>2</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>2</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행할 경우 성공 가능성이 높다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Ltd</td><td>0.9</td><td>이메일을 열람하는 일반적인 동작이 필요하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>희생자에게 메일을 보냄으로써 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>M</td><td>0.9</td><td>외부 입력에 대한 필터링 코드를 추가하여야 하며, 이는 하나의 지점이 아님 복수의 지점일 것으로 판단되므로 M으로 판정한다. CSRF역시 중간 정도 이상의 수정이 필요하다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>M</td><td>0.7</td><td>XSS에 대한 일반적인 방어방법이 존재하나, 지식을 가진 공격자의 노력에 의해서 침해가 발생할 수 있다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">55.22</td></tr>
</table>

26. [13-021] 워드프로세서 소프트웨어 Integer Overflow 취약점 #1

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>정수 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행할 경우 성공 가능성이 매우 높다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Mod</td><td>0.8</td><td>희생자의 출퍼가 불분명한 한글 파일을 여는 협조적인 행동이 필요하므로 M으로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>취약한 한글 파일을 희생자에게 전달하면 되므로 특별한 권한은 필요하지 않다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	L	0.8	정수 넘침이 발생하는지 여부를 검사하는 코드를 추가하면 되므로 제한된 코드의 추가만이 필요할 것으로 판정된다.
외부 제어의 효과 (EC)	N	1.0	해당 취약점을 방어/완화하기 위한 외부 제어 방법은 없다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	79.03		

27. [13-022] 백신 자체보호 기능 우회 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점을 가지는 소프트웨어는 가장 널리 사용되는 보안 프로그램이므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	V3Lite 작동중지로 사용 PC가 악성코드에 노출됨에 따라 어느 정도 물적 손실이나 자산 손실이 있을 수 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>2</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>2</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>D</td><td>0.6</td><td>레지스트리 변경에 대한 자체 보호기능의 약점에 대한 것으로 이 부분에 대한 침해 가능성은 해당 바이러스의 전파에 따라 유동적이고 해당 취약성과는 직접적인 연관은 없다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>L</td><td>0.9</td><td>바이러스 전파에 대한 피해자의 상호 작용 정도는 피해자의 일반적인 활동으로도 가능하므로 L로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>바이러스 전파의 경우 특별한 권한 없이 침해를 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>M</td><td>0.9</td><td>복수개의 모듈에 대한 수정이 필요한 것으로 판단되므로 M으로 판정한다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>바이러스의 레지스트리 설정과 관련한 특별한 외부 제어는 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">79.36</td></tr>
</table>

28. [13-045] 워드프로세서 소프트웨어 스택 오버플로우 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>스택 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 한컴 오피스에 대하여, 해당 파일을 수행할 경우 침해가 발생할 확률이 높음</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 공격 파일을 전달하여 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>M</td><td>0.8</td><td>희생자가 출처가 불분명한 한글 파일을 열어보는 위험한 행동을 수행하여야 하므로 M으로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	L	0.8	버퍼 넘침이 발생하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.
외부 제어의 효과 (EC)	I	0.5	ASRL 방법이 존재하나, 부분적인 방어만 가능하다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	39.51		

29. [13-050] 워드프로세서 소프트웨어 힙 오버플로우

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	힙 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.
기술적 영향 (TI)			TI 항목 / 점수 Modify data (2/1/0) 0 Read data (2/1/0) 0 DoS: unreliable execution (2/1/0) 0 DoS: resource consumption (2/1/0) 0 Execute unauthorized code or commands (4/2/0) 4 Gain privileges / assume identity (2/1/0) 0 Bypass protection mechanism (2/1/0) 0 Hide activities (2/1/0) 0 합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N 4

평가항목	평가결과		평가 근거
침해 가능성 (EX)	H	1.0	취약점을 가진 한글 프로그램이 해당 파일을 수행할 경우 침해가 발생할 확률이 높음
접근 벡터 (AV)	I	1.0	일반적인 인터넷을 통해 공격 파일을 전달하여 침해가 가능하므로 I로 판단한다.
상호작용 정도 (IN)	M	0.8	희생자가 출처가 불분명한 한글 파일을 열어보는 위험한 행동을 수행하여야 하므로 M으로 판정한다.
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
수정 난이도 (RE)	L	0.8	버퍼 할당 크기를 결정하는 부분과 저장 부분의 코드의 수정만 필요할 것으로 판단된다.
외부 제어의 효과 (EC)	I	0.5	ASRL 방법이 존재하나, 부분적인 방어만 가능하다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	39.51		

30. [13-056] 메신저 프로그램 세션 노출 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점을 가지는 해당 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	3천만 사용자를 갖고 있으므로 세션 노출만으로도 상당한 사회적 손실의 가능성이 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>2</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행하고, 희생자가 협조적인 동작을 할 경우 성공 가능성이 매우 높음.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>R</td><td>0.8</td><td>프록시 서버 접근을 위하여 같은 내부 네트워크 안에 위치하여야 한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Ltd</td><td>0.9</td><td>희생자가 플러스 친구에게 접속하는 일반적인 동작을 수행하여야 한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>L</td><td>0.8</td><td>관련 통신을 SSL로 수행하도록 수정하는 코드를 추가하여야 할 것으로 판단되며, 이는 제한적인 범위가 될 것이다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>이 취약점을 위한 특별한 외부 제어 방법은 없다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">71.02</td></tr>
</table>

31. [13-057] 홈페이지 구축 소프트웨어 XSS 취약점 #3

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>C</td><td>0.8</td><td>해당 취약점을 가지는 소프트웨어는 PHP에 기반을 둔 공개 소프트웨어로 널리 알려진 응용 소프트웨어에 해당하므로 Common으로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>스크립트 실행으로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>2</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>2</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 취약한 사이트에 위험한 스크립트를 업로드 하는 것이 어렵지 않고 성공 가능성이 높은 것으로 판단하여 H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Ltd</td><td>0.9</td><td>게시물에 접근하는 일반적인 동작이 필요하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>G</td><td>0.9</td><td>임베드 태그 설정 및 스크립트 업로드를 위한 게스트 수준의 회원 가입이 필요하다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	L	0.8	해당 태그 설정 및 스크립트 수행에 대한 필터링 관련 코드만 수정하면 된다.
외부 제어의 효과 (EC)	M	0.7	XSS에 대한 일반적인 방어방법이 존재하나, 지식을 가진 공격자의 노력에 의해서 침해가 발생할 수 있다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	56.06		

32. [13-092] 홈페이지 구축 소프트웨어 원격 코드 실행

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>C</td><td>0.8</td><td>제로보드는 널리 알려진 응용 소프트웨어에 해당하므로 Common으로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>원격 코드 공격을 이용하여 정보를 유출 혹은 조작할 수 있으므로 중요한 물적 손실이 발생할 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
</table>

평가항목	평가결과		평가 근거
침해 가능성 (EX)	H	1.0	외부에서 취약한 소프트웨어에 접근하여 공격을 수행할 경우 해당 디렉토리에 공격 스크립트를 복사하여야 하는데, 이 과정의 성공 확률이 가변적이다.
접근 벡터 (AV)	I	1.0	일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.
상호작용 정도 (IN)	N	1.0	희생자의 협조적 행동은 필요 없다.
권한 요구도 (RP)	N	1.0	특별한 회원가입 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
수정 난이도 (RE)	L	0.8	widgets/$widget 디렉토리에 대한 파일 생성 권한을 제약함으로서 침해를 방지할 수 있다.
외부 제어의 효과 (EC)	N	1.0	희생자의 잘못된 수행에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	82.56		

33. [13-105] 금융권 ActiveX 원격 코드 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 취약점이 발견되는 소프트웨어는 가장 널리 사용되는 보안 관련 소프트웨어에 해당되므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	H	0.9	nProtect Netizen은 금융권, 공공기관, 전자결제 등 대다수의 대형 사이트에 공급된 온라인 보안 솔루션으로 원격 코드 공격으로 인해 사회적으로 높은 수준의 피해가 발생할 잠재성을 갖고 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>C</td><td>1.0</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>1</td></tr>
<tr><td>Read data (2/1/0)</td><td>1</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>6</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 약점을 가진 피해자는 공격 사이트에 접속시 침해당할 가능성이 높으므로 H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Ltd</td><td>0.9</td><td>인터넷 접속을 통해 침해가 발생하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>M</td><td>0.9</td><td>복수개의 관련 모듈에 대한 수정이 요구된다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>희생자의 잘못된 접근에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">93.56</td></tr>
</table>

34. [13-108] 워드프로세서 소프트웨어 Integer Overflow 취약점 #2

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>W</td><td>1.0</td><td>해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>정수 오버플로우 발생 가능하지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 약간의 물적 손실이나 자산 손실이 있을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행할 경우 성공 가능성이 매우 높다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 공격 파일을 전송하여 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Mod</td><td>0.8</td><td>희생자의 출퍼가 불분명한 한글 파일을 여는 협조적인 행동이 필요하므로 M으로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>취약한 한글 파일을 희생자에게 전달하면 되므로 특별한 권한은 필요하지 않다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	L	0.8	정수 넘침이 발생하는지 여부를 검사하는 코드를 추가하면 되므로 제한된 코드의 추가만이 필요할 것으로 판정된다.
외부 제어의 효과 (EC)	N	1.0	해당 취약점을 방어/완화 하기 위한 외부 제어 방법은 없다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	79.03		

35. [13-109] 동영상 플레이어 원격코드 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점을 가지는 곰플레이어 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	곰플레이어 원격 코드 실행 가능성이 보고된 수준으로 중간 정도의 피해 잠재성을 갖고 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>2</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 취약한 곰플레이어가 설치된 사용자는 크롬을 사용하여 위험한 웹사이트 접속시 침해 가능성이 높다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Ltd</td><td>0.9</td><td>일반적인 웹페이지 접근 및 곰플레이어 설치에 의하여 침해가 발생하므로 Ltd로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한은 요구하지 않는다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>L</td><td>0.8</td><td>외부 경로값에 대한 검사를 수행하는 제한된 범위의 수정이 필요하다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>특별히 해당 취약성에 대한 외부 제어 방법은 없다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>LT</td><td>0.8</td><td>해당 보안 취약점은 존재하나 공격방식 및 성공가능 여부가 명확하지 않으므로 Proven Locally True 로 판정한다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">70.49</td></tr>
</table>

36. [13-117] 압축 프로그램 Directory Traversal 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>L</td><td>0.6</td><td>해당 보안 취약점을 가지는 반디집 소프트웨어는 사용자가 제한적인 소프트웨어에 해당하므로 Limited로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>L</td><td>0.7</td><td>일부 경로에 대한 시스템 무결성에 영향을 줌으로써 낮은 정도의 피해 잠재성을 갖고 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>C</td><td>1.0</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>1</td></tr>
<tr><td>Read data (2/1/0)</td><td>1</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>6</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>M</td><td>0.6</td><td>해당 공격이 시행될 경우 해당 파일의 대치 등에 대한 경고 문자열이 나올 수 있고, 해당 파일 경로가 표시되므로 이에 대하여 희생자가 인지할 수 있으므로, 침해 가능성은 가변적이다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 위험한 압축파일을 전달하여 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>M</td><td>0.8</td><td>희생자가 출처가 불분명한 압축 파일을 열어보는 위험한 행동을 수행하여야 하므로 M으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
권한 요구도 (RP)	N	1.0	특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.
수정 난이도 (RE)	L	0.8	경로병을 검사하는 부분에 대한 코드의 수정만 필요할 것으로 판단된다.
외부 제어의 효과 (EC)	N	1.0	해당 취약점에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	70.56		

37. [13-122] 워드프로세서 소프트웨어 Signed Extension Error Handling 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	W	1.0	해당 보안 취약점을 가지는 한컴오피스의 한글 소프트웨어는 가장 널리 사용되는 응용 소프트웨어에 해당하므로 Widespread로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	L	0.7	메모리 주소 값을 변경할 수 있지만 악성 코드 유포 및 실행 메커니즘을 제시하지 않았으므로 낮은 수준의 물적 손실이나 자산 손실이 있을 수 있음.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점을 가진 시스템에 대하여 제시된 공격방법을 시행할 경우 성공 가능성이 매우 높다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>M</td><td>0.8</td><td>희생자의 출퍼가 불분명한 한글 파일을 여는 협조적인 행동이 필요하므로 M으로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>취약한 한글 파일을 희생자에게 전달하면 되므로 특별한 권한은 필요하지 않다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>L</td><td>0.8</td><td>음수일 경우를 처리하는 오류 처리 코드를 삽입하면 되므로 제한적인 수정만이 요구된다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>해당 취약점을 방어/완화 하기 위한 외부 제어 방법은 없다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">79.03</td></tr>
</table>

38. [13-131] 웹에디터 소스코드 파일 다운로드 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>C</td><td>0.8</td><td>해당 보안 취약점이 발견되는 나모 크로스에디터는 널리 알려진 응용 소프트웨어에 해당하므로 Common으로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>소스 코드 정보를 유출 혹은 조작할 수 있으므로 중간 정도의 물적 손실이 발생할 가능성이 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><td>TI 항목</td><td>점수</td></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>2</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>1</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>3</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>침해가 발생할 확률이 높으며, 간단한 공격 방법이 제시되어 있으므로, H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적 행동이 필요없으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	L	0.8	외부 입력 이미지 경로명에 대한 검증 코드만 추가하면 된다.
외부 제어의 효과 (EC)	N	1.0	해당 부적절한 경로명 전달에 대한 외부 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	72.24		

39. [13-162] 웹서버 프로그램 원격 코드 실행 취약점

평가항목	평가결과		평가 근거
출현 빈도 (P)	H	0.9	해당 보안 취약점이 발견되는 Struts2는 웹서비스 개발에 널리 사용되는 시스템 소프트웨어이므로 High로 판정한다.
적용 범위 (SC)	A	1.0	해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.
산업적 영향 (BI)	M	0.8	웹쉘 코드 공격을 이용하여 정보를 유출 혹은 조작할 수 있으므로 중요한 물적 손실이 발생할 수 있으며 또한 해당 서버를 이용하여 내부망의 pc를 쉽게 공격할 수 있기 때문에 피해가 확산될 수 있음.현재 패치가 제공됨.

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적 영향 (TI)</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>4</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>0</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점이 알려져 있으며, 취약한 소프트웨어를 사용할 경우 침해가 발생할 확률이 높으므로, H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요없으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
<tr><td>수정 난이도 (RE)</td><td>L</td><td>0.8</td><td>외부 입력에 대한 검증 코드만 추가하면 된다.</td></tr>
<tr><td>외부 제어의 효과 (EC)</td><td>N</td><td>1.0</td><td>해당 부적절한 인자값 전달에 대한 외부적인 제어 방법은 특별히 없으므로 N으로 판정한다.</td></tr>
<tr><td>보고의 신뢰성 (FC)</td><td>T</td><td>1.0</td><td>해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.</td></tr>
<tr><td>중요도 점수</td><td colspan="3">84.00</td></tr>
</table>

40. [13-175] DVR 장비 관리자 페이지 인증 우회 취약점

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>출현 빈도 (P)</td><td>L</td><td>0.6</td><td>해당 보안 취약점이 존재하는 삼성 DVR 웹뷰어 소프트웨어는 사용자가 많지 않은 제한적인 소프트웨어에 해당하므로 Limited로 판정한다.</td></tr>
<tr><td>적용 범위 (SC)</td><td>A</td><td>1.0</td><td>해당 보안 취약점이 대상 시스템이 인스톨되는 모든 플랫폼과 설정에 존재하는 경우이다.</td></tr>
<tr><td>산업적 영향 (BI)</td><td>M</td><td>0.8</td><td>DVR 내에 저장된 파일의 손상으로 인해 중간 정도의 물적 손실이나 자산 손실의 결과를 낳을 수 있음.</td></tr>
<tr><td>기술적 영향 (TI)</td><td>M</td><td>0.6</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>0</td></tr>
<tr><td>Read data (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>2</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>0</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>취약점이 알려져 있으며, 취약한 소프트웨어를 사용할 경우 침해가 발생할 확률이 높으므로, H로 판정한다.</td></tr>
<tr><td>접근 벡터 (AV)</td><td>I</td><td>1.0</td><td>일반적인 인터넷을 통해 침해가 가능하므로 I로 판단한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Aut</td><td>1.0</td><td>희생자의 협조적인 행동이 필요 없으므로 Aut로 판정한다.</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>특별한 권한 없이 침해 공격을 수행할 수 있으므로 N으로 판정한다.</td></tr>
</table>

평가항목	평가결과		평가 근거
수정 난이도 (RE)	M	0.9	외부에서 전달된 쿠키에 대한 검사 코드 및 암호화하여 계정정보를 저장하는 코드를 추가하여야 하므로 복수 모듈으 중간정도 수정이 필요하다.
외부 제어의 효과 (EC)	N	1.0	해당 침해에 대한 외부적인 제어 방법은 특별히 없으므로 N으로 판정한다.
보고의 신뢰성 (FC)	T	1.0	해당 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하는 경우이다.
중요도 점수	70.14		

제 3 절 시범평가 결과

1. 평가 항목별 점수

[표 4-1]의 40개 취약점에 대한 CWSS 방법론을 이용한 평가항목별 평가 결과는 [표 4-2]와 같이 요약할 수 있다.

[표 4-2] 평가 항목별 점수

	P	SC	BI	TI	EX	IN	AV	RP	RE	EC	FC	Score
12-011	1.00	1.00	0.80	0.90	1.00	1.00	1.00	1.00	0.90	0.90	1.00	77.33
12-014	1.00	0.90	0.70	0.90	0.20	0.75	0.30	0.80	0.80	1.00	1.00	53.57
12-016	1.00	1.00	0.90	0.60	1.00	1.00	1.00	1.00	0.90	1.00	1.00	79.38
12-019	0.90	1.00	0.70	0.90	0.60	1.00	0.30	1.00	0.80	1.00	1.00	63.16
12-023	1.00	0.70	0.70	0.90	1.00	0.75	0.10	0.80	0.80	1.00	1.00	56.04
12-029	1.00	0.50	0.70	0.90	1.00	1.00	1.00	1.00	0.80	0.90	1.00	65.32
12-034	0.80	1.00	0.90	0.90	1.00	1.00	1.00	0.60	0.80	0.90	1.00	72.33
12-052	0.90	1.00	0.80	0.90	1.00	1.00	0.90	1.00	0.90	1.00	1.00	82.79
12-064	1.00	1.00	0.80	0.90	1.00	1.00	0.80	1.00	0.80	1.00	1.00	82.02
12-071	0.60	1.00	0.70	0.90	0.60	0.75	0.90	0.80	0.90	1.00	1.00	63.68
12-072	1.00	1.00	0.70	0.90	1.00	1.00	0.80	1.00	0.80	1.00	1.00	77.41

	P	SC	BI	TI	EX	IN	AV	RP	RE	EC	FC	Score
12-075	1.00	1.00	0.70	0.90	1.00	1.00	0.80	1.00	0.80	1.00	1.00	77.41
12-084	0.60	1.00	0.80	0.60	1.00	1.00	1.00	1.00	0.80	1.00	1.00	69.72
12-094	1.00	1.00	0.70	0.90	1.00	1.00	0.90	1.00	0.80	1.00	1.00	79.03
12-103	0.60	1.00	0.70	0.60	1.00	1.00	1.00	1.00	0.90	1.00	1.00	65.94
12-109	0.80	1.00	0.80	0.90	1.00	1.00	0.90	0.90	0.90	0.50	1.00	39.86
12-129	1.00	1.00	0.00	0.30	0.20	1.00	0.80	1.00	0.80	1.00	0.00	0.00
12-131	0.80	0.50	0.70	0.90	1.00	1.00	1.00	1.00	0.80	0.70	1.00	48.99
12-135	1.00	1.00	0.70	0.90	1.00	1.00	0.80	1.00	0.90	1.00	1.00	77.88
12-159	1.00	1.00	0.90	0.90	1.00	1.00	0.90	0.90	0.90	1.00	1.00	87.09
12-163	0.60	1.00	0.80	0.60	1.00	1.00	1.00	1.00	0.90	1.00	1.00	70.14
12-165	1.00	1.00	0.70	0.60	1.00	1.00	1.00	1.00	0.90	1.00	1.00	70.98
13-002	0.80	1.00	0.70	0.90	1.00	0.90	1.00	0.90	0.80	0.70	1.00	52.80
13-005	1.00	1.00	0.80	0.90	1.00	1.00	1.00	1.00	0.90	1.00	1.00	85.92
13-020	0.90	1.00	0.70	0.90	1.00	0.90	1.00	1.00	0.90	0.70	1.00	55.22
13-021	1.00	1.00	0.70	0.90	1.00	0.80	1.00	1.00	0.80	1.00	1.00	79.03
13-022	1.00	1.00	0.80	0.90	0.60	0.90	1.00	1.00	0.90	1.00	1.00	79.36
13-045	1.00	1.00	0.70	0.90	1.00	0.80	1.00	1.00	0.80	0.50	1.00	39.51
13-050	1.00	1.00	0.70	0.90	1.00	0.80	1.00	1.00	0.80	0.50	1.00	39.51
13-056	1.00	1.00	0.80	0.60	1.00	0.90	0.80	1.00	0.80	1.00	1.00	71.02
13-057	0.80	1.00	0.80	0.90	1.00	0.90	1.00	0.90	0.80	0.70	1.00	56.06
13-092	0.80	1.00	0.80	0.90	1.00	1.00	1.00	1.00	0.80	1.00	1.00	82.56
13-105	1.00	1.00	0.90	1.00	1.00	0.90	1.00	1.00	0.90	1.00	1.00	93.56
13-108	1.00	1.00	0.70	0.90	1.00	0.80	1.00	1.00	0.80	1.00	1.00	79.03
13-109	1.00	1.00	0.80	0.60	1.00	0.90	1.00	1.00	0.80	1.00	0.80	70.49
13-117	0.60	1.00	0.70	1.00	0.60	0.80	1.00	1.00	0.80	1.00	1.00	70.56
13-122	1.00	1.00	0.70	0.90	1.00	0.80	1.00	1.00	0.80	1.00	1.00	79.03
13-131	0.80	1.00	0.80	0.60	1.00	1.00	1.00	1.00	0.80	1.00	1.00	72.24
13-162	0.90	1.00	0.80	0.90	1.00	1.00	1.00	1.00	0.80	1.00	1.00	84.00
13-175	0.60	1.00	0.80	0.60	1.00	1.00	1.00	1.00	0.90	1.00	1.00	70.14

[표 4-3]에서는 40개 보안 취약점에 대한 시범 평가 결과를 점수 순으로 정렬하였다. 보다 높은 점수를 받을수록 보안 취약점의 위험도가 높다고 판단된다.

[표 4-3] 보안 취약점 평가결과 (점수순)

번호	보안 취약점 이름	점수
13-105	nProtect Netizen v5.5 원격 코드 실행 취약점	93.56
12-159	Adobe Flash Player 취약점	87.09
13-005	메신저 프로그램 계정 탈취 취약점	85.92
13-162	Struts2원격코드실행취약점	84.00
13-092	ZeroBoard XE Remote Code Execution	82.56
12-064	정부부처 겨냥한 한글 제로데이 공격 시도	82.02
12-016	CiscoNX-OS서비스거부	79.38
13-022	AhnLab V3 Lite 자체보호 취약점	79.36
12-094	곰플레이어 힙 오버플로우	79.03
13-021	한컴 오피스 한글 2010 SE+의 이미지 파싱 모듈 정수 오버플로우 취약점	79.03
13-108	한글 2010 정수 오버플로우	79.03
13-122	한컴 오피스 한글 2010 SE Signed extension error handling 취약점	79.03
12-052	삼성 Kies 원격코드 실행	78.56
12-135	네이트온 이미지 파일 공유	77.88
12-072	한글 2010 힙 오버플로우 0-day 취약점	77.41
12-075	미리보기 내용 기반 한글 버퍼넘침	77.41
12-011	PHP 원격코드 실행 취약점	77.33
12-034	XpressEngine 웹쉘코드 삽입	72.33
13-131	Namo CrossEditor2 웹 소스코드 파일 다운로드 취약점	72.24
13-056	메신저 프로그램 세션 노출 취약점	71.02
12-165	한국사이버결제 주요 개인정보 노출 취약점	70.98
13-117	반디집 Directory Traversal 취약점	70.56

번호	보안 취약점 이름	점수
13-109	곰플레이어 원격 코드 실행 취약점	70.49
12-163	더존 그룹웨어 및 회계관리 DB 시스템 취약점	70.14
13-175	Samsung DVR Vulnerability	70.14
12-084	LG 에어컨 관리자 페이지 취약점	69.72
12-103	NAS 관리자 페이지 계정정보 유출 취약점	65.94
12-029	PHP-CGI 소스코드 노출	65.32
12-071	초코플레이어 DLL하이제킹	63.68
12-019	Netsarang Xshell 임의코드 실행	59.44
13-057	공개용 게시판(제로보드, Wordpress, Textcube) XSS 취약점	56.06
12-023	곰플레이어 2.1.37 버퍼넘침	56.04
13-020	ipTIME 유무선 공유기 CSRF XSS 취약점	55.22
13-002	제로보드 XE 1.5.4 Ver XSS 취약점	52.80
12-014	알FTP 로컬 파일 실행	51.34
12-131	그누보드 SQL 삽입 취약점	48.99
12-109	그누보드4 XSS 취약점	39.86
13-045	한컴 오피스 2010 SE 스택 오버플로우 취약점	39.51
13-050	워드프로세서 소프트웨어 힙 오버플로우	39.51
12-129	Acrobat Reader 취약점	0.00

2. CWSS 평가점수 계산

본 절에서는 항목별 평가 점수를 이용해서 CWSS 점수를 계산하는 방식에 대하여 설명한다.

CWSS 버전 0.6의 평가 점수는 0부터 100 사이의 숫자로 표현되며, 이 점수는 (Base Finding 점수) * (Attack Surface 점수) * (Environmental 점

수) 라는 기본 공식을 이용하여 계산된다. Base Finding 점수는 0부터 100 사이의 점수를 가지며, Attack Surface 점수와 Environmental 점수는 0부터 1 사이의 값을 가지게 된다.

CWSS의 영역별 점수는 다음과 같은 공식을 이용하여 계산한다.

*CWSS score = (Base Finding) * (Attack Surface) * (Environmental)*

*Base Finding 점수 = { (10*TI + 5*(AP+AL) + 5*FC) * f(TI) * IC } * 4.0*

이 공식은 취약점의 기본적인 특성과 관련된 항목들의 점수를 100점 만점으로 계산한다. 이 공식에서 사용되는 f(TI)의 값은 가중치로 만약 TI가 0으로 평가된 경우에는 0을, 그 외의 경우에는 1을 값으로 가진다. 이는 어떤 취약점의 기술적 영향도가 0으로 평가된 경우에는 다른 요소들의 값에 관계없이 Base Finding 부분점수가 0으로 평가된다는 것을 의미한다. 본 시범평가에서는 Base Finding 그룹에 속한 메트릭 중에서 AP, AL, IC 항목이 사용되지 않았으며, 점수 계산 시 이 항목들은 1로 처리하였다.

Attack Surface 점수 = {20(RP+RL+AV) + 20*SC + 10*IN + 5*(AS+AI)} / 100.0*

이 공식은 공격유형 및 난이도와 관련된 항목들의 점수를 100점 만점으로 계산하여 다시 0부터 1사이의 값으로 정규화하는데 사용된다. 본 시범평가에서는 Attack Surface 그룹에 속한 메트릭 중에서 RL, AS, AI 항목이 사용되지 않았으며, 점수 계산 시 이 항목들은 1로 처리하였다.

*Environmental 점수 = { (10*BI + 3*(DI+EX) +3*P + RE) * f(BI) * EC } / 20.0*

이 공식은 환경적 영향과 관련된 항목들의 점수를 20점 만점으로 계산

하여 다시 0부터 1사이의 값으로 정규화하는데 사용된다. 이 공식에서 사용되는 f(BI)의 값은 가중치로 만약 BI가 0으로 평가된 경우에는 0을, 그 외의 경우에는 1을 값으로 가진다. 이는 어떤 취약점의 산업적 영향도가 0으로 평가된 경우에는 다른 요소들의 값에 관계없이 Environmental 부분점수가 0으로 평가된다는 것을 의미한다. 본 시범평가에서는 Environmental 그룹에 속한 메트릭 중에서 DI 항목이 사용되지 않았으며, 점수 계산 시 이 항목은 1로 처리하였다.

3. 평가 결과 분석

본 절에서는 [표 4-3]에 명시된 국내 취약점에 대한 CWSS 시범평가 결과를 CWSS에서 사용하는 대분류에 따라 기술적인 영향, 공격방식의 유형, 환경적인 영향으로 나누어 분석해 본다. [표 4-4]는 각 보안 취약점의 평가 영역별 점수를 보여주고 있다.

[표 4-4] 평가 영역별 부분 점수

	Base Finding	Attack Surface	Environmental	Score
12-011	96.00	1.00	0.81	77.33
12-014	96.00	0.78	0.72	53.57
12-016	84.00	1.00	0.95	79.38
12-019	96.00	0.86	0.77	63.16
12-023	96.00	0.70	0.84	56.04
12-029	96.00	0.90	0.76	65.32
12-034	96.00	0.92	0.82	72.33
12-052	96.00	0.98	0.88	82.79
12-064	96.00	0.96	0.89	82.02
12-071	96.00	0.92	0.73	63.68
12-072	96.00	0.96	0.84	77.41
12-075	96.00	0.96	0.84	77.41
12-084	84.00	1.00	0.83	69.72

	Base Finding	Attack Surface	Environmental	Score
12-094	96.00	0.98	0.84	79.03
12-103	84.00	1.00	0.79	65.94
12-109	96.00	0.96	0.43	39.86
12-129	52.00	0.96	0.00	0.00
12-131	96.00	0.90	0.57	48.99
12-135	96.00	0.96	0.85	77.88
12-159	96.00	0.96	0.95	87.09
12-163	84.00	1.00	0.84	70.14
12-165	84.00	1.00	0.85	70.98
13-002	96.00	0.97	0.57	52.80
13-005	96.00	1.00	0.90	85.92
13-020	96.00	0.99	0.58	55.22
13-021	96.00	0.98	0.84	79.03
13-022	96.00	0.99	0.84	79.36
13-045	96.00	0.98	0.42	39.51
13-050	96.00	0.98	0.42	39.51
13-056	84.00	0.95	0.89	71.02
13-057	96.00	0.97	0.60	56.06
13-092	96.00	1.00	0.86	82.56
13-105	100.00	0.99	0.95	93.56
13-108	96.00	0.98	0.84	79.03
13-109	80.00	0.99	0.89	70.49
13-117	100.00	0.98	0.72	70.56
13-122	96.00	0.98	0.84	79.03
13-131	84.00	1.00	0.86	72.24
13-162	96.00	1.00	0.88	84.00
13-175	84.00	1.00	0.84	70.14

가. 기술적인 영향

보안 취약점들이 공격에 이용되었을 때 희생자 시스템에 미치는 영향

의 심각성과 약점 보고의 정확도를 반영하는 평가 영역이다.

평가 결과를 분석해 보면 시범 평가에 사용된 국내 보안 취약점들은 버퍼 넘침 오류를 이용한 임의코드 실행이 가장 보편적인 방식으로 사용되고 있음을 보여주고 있다. 이는 CWSS에서 매우 심각한 것으로 분류하고 있는 취약점으로 결과적으로 Base Finding 부분점수가 대부분 비슷한 수준을 보이고 있는 것을 알 수 있다. 그 외에 패스워드의 평문 저장(12-084)이나 서비스 거부공격 (12- 016) 등의 공격은 Base Finding 부분점수가 상대적으로 낮게 평가되었다.

[표 4-5]는 시범 평가에 사용된 국내 보안 취약점을 기술적인 영향 분류의 평가 점수에 따라서 정렬한 결과를 보여주고 있다.

[표 4-5] "기술적인 영향"평가결과 (점수순)

번호	영역 점수	최종 점수
13-105	100.00	93.56
13-117	100.00	70.56
12-011	96.00	77.33
12-014	96.00	51.34
12-019	96.00	59.44
12-023	96.00	56.04
12-029	96.00	65.32
12-034	96.00	72.33
12-052	96.00	78.56
12-064	96.00	82.02
12-071	96.00	63.68
12-072	96.00	77.41

12-075	96.00	77.41
12-094	96.00	79.03
12-109	96.00	39.86
12-131	96.00	48.99
12-135	96.00	77.88
12-159	96.00	87.09
13-002	96.00	52.80
13-005	96.00	85.92
13-020	96.00	55.22
13-021	96.00	79.03
13-022	96.00	79.36
13-045	96.00	39.51
13-050	96.00	39.51
13-057	96.00	56.06
13-092	96.00	82.56
13-108	96.00	79.03
13-122	96.00	79.03
13-162	96.00	84.00
12-016	84.00	79.38
12-084	84.00	69.72
12-103	84.00	65.94
12-163	84.00	70.14
12-165	84.00	70.98
13-056	84.00	71.02
13-131	84.00	72.24
13-175	84.00	70.14

13-109	80.00	70.49
12-129	52.00	0.00

나. 공격방식의 유형

보안 취약점을 이용한 공격의 발견난이도와 성공난이도를 평가하는 항목으로 간단한 쿼리만으로 공격이 가능한 취약점들(12-016, 12-084, 12-103)이 상대적으로 높은 Attack Surface 부분점수를 보이고 있다.

[표 4-6]은 시범 평가에 사용된 국내 보안 취약점을 공격방식의 유형 분류의 평가 점수에 따라서 정렬한 결과를 보여주고 있다.

[표 4-6]

"공격유형"평가결과

(점수순)

번호	영역 점수	최종 점수
12-011	1.00	77.33
13-005	1.00	85.92
13-092	1.00	82.56
13-162	1.00	84.00
12-016	1.00	79.38
12-084	1.00	69.72
12-103	1.00	65.94
12-163	1.00	70.14
12-165	1.00	70.98
13-131	1.00	72.24
13-175	1.00	70.14

13-105	0.99	93.56
13-020	0.99	55.22
13-022	0.99	79.36
13-109	0.99	70.49
13-117	0.98	70.56
12-052	0.98	78.56
12-094	0.98	79.03
13-021	0.98	79.03
13-045	0.98	39.51
13-050	0.98	39.51
13-108	0.98	79.03
13-122	0.98	79.03
13-002	0.97	52.80
13-057	0.97	56.06
12-064	0.96	82.02
12-072	0.96	77.41
12-075	0.96	77.41
12-109	0.96	39.86
12-135	0.96	77.88
12-159	0.96	87.09
12-129	0.96	0.00
13-056	0.95	71.02
12-034	0.92	72.33
12-071	0.92	63.68
12-029	0.90	65.32
12-131	0.90	48.99

12-019	0.86	59.44
12-014	0.78	51.34
12-023	0.70	56.04

다. 환경적인 영향

환경적인 영향 영역은 보안 취약점을 가진 시스템이 전체 시스템 환경에 미치는 영향을 평가하고, 동시에 보안 취약점의 심각성에 영향을 미치는 환경적인 조건을 평가하는 항목이다.

평가 결과를 분석해 보면 시범 평가에 사용된 국내 보안 취약점들 중에서사용자가 많은 PHP 스크립트 언어나 아래한글, Adobe Flash Player 등이 환경적인 영향 영역점수에서 상대적으로 높게 평가된 것을 알 수 있다. 이에 비하여 사용자가 제한적인 소프트웨어 (그누보드, 초코플레이어 등)는 낮은 환경적인 영향도를 보이고 있다. 또한 보안 취약점 12-129의 경우에는 사용자가 매우 많은 Adobe reader의 약점에도 불구하고 실제로 해당 보안 취약점을 공격에 이용할 수 있는 방법이 현재까지는 보고되지 않은 경우로 BI가 0으로 평가되었고, 결과적으로 환경적인 영향 영역점수 역시 0으로 평가되었다.

또한 아래한글과 관련된 보안 취약점 중에서 13-045와 13-050의 경우에는 ASRL(Address Space Layout Randomization) 기법을 이용하여 부분적인 방어가 가능하여 환경적인 영향 영역점수가 상대적으로 낮게 평가되었으며, 그 결과가 보안 취약점 최종점수에도 영향을 준 것을 알 수 있다.

[표 4-7]은 시범 평가에 사용된 국내 보안 취약점을 환경적인 영향 분류의 평가 점수에 따라서 정렬한 결과를 보여주고 있다.

[표 4-7] “환경적인 영향”평가결과 (점수순)

번호	영역 점수	최종 점수
12-016	0.95	79.38
13-105	0.95	93.56
12-159	0.95	87.09
13-005	0.90	85.92
13-109	0.89	70.49
12-064	0.89	82.02
13-056	0.89	71.02
13-162	0.88	84.00
13-092	0.86	82.56
13-131	0.86	72.24
12-165	0.85	70.98
12-135	0.85	77.88
12-094	0.84	79.03
13-021	0.84	79.03
13-108	0.84	79.03
13-122	0.84	79.03
12-072	0.84	77.41
12-075	0.84	77.41
12-023	0.84	56.04
12-163	0.84	70.14
13-175	0.84	70.14
13-022	0.84	79.36

12-052	0.84	78.56
12-084	0.83	69.72
12-034	0.82	72.33
12-011	0.81	77.33
12-103	0.79	65.94
12-029	0.76	65.32
12-071	0.73	63.68
13-117	0.72	70.56
12-019	0.72	59.44
12-014	0.69	51.34
13-057	0.60	56.06
13-020	0.58	55.22
13-002	0.57	52.80
12-131	0.57	48.99
12-109	0.43	39.86
13-045	0.42	39.51
13-050	0.42	39.51
12-129	0.00	0.00

제 5 장 소프트웨어 대상 신규 취약점 평가방법 연구

제 1 절 서론

본 절에서는 신규 취약점 보고의 중요도 및 보안 취약점 자체의 중요도 평가를 위한 평가 체계 연구 내용을 기술한다. 평가 체계의 개발을 수행함에 있어 다음과 같은 방법론을 설정하고 연구를 진행하였다.

- o 취약점 발굴 포상을 위한 평가를 위한 중요도 점수(이하 취약점 발굴 점수) 및 취약점 데이터베이스 구축을 위한 중요도 점수(이하 취약점 DB 점수)의 계산 방법을 목적에 부합하도록 각각 개발한다.
- o 평가척도간의 중복성 및 의존성을 최대한 배제한다. 이를 위하여 주요 평가 요소를 우선 설정하고 각 요소별 평가 척도를 설정한다.
- o 평가의 객관성 및 용이성을 고려하여 객관적 기준을 제시하고, 과다한 평가 척도의 사용을 지양한다.

이를 위하여 기존의 평가 척도에 대한 분석과 시범 평가에 대한 1차적인 분석 결과에 기반하여 본 평가 방법의 목적에 부합하는 개선된 평가 방법을 개발하고자 하였다. 또한, 기존에 사용되고 있는 취약점 포상제를 위한 평가방법을 분석하여, 새로운 평가 방법 개발에 반영하였다.

본 장에서는 평가 척도의 선정까지의 작업과 결정과정에 대하여 기술하고, 이러한 평가 척도에 대한 점수 부여 방법 및 최종 점수 도출 방법을 설명한다. 또한 한국인터넷진흥원에서 제공한 40개 취약점 보고 사례에 대하여 본 연구에서 개발한 취약점 평가방법을 사용한 시범평가 결과를 제시한다.

제 2 절 기존 보안 취약점 및 보안약점 평가 방법 개요

1. 기존 평가 방법론의 특징 분석

본 절에서는 CWSS, CVSS 및 기존의 인터넷진흥원에서 사용하고 있는 취약점 발굴 포상제 평가 방법의 특징을 기술한다.

CVSS는 보안 취약점을 위한 평가척도로서, 이미 알려진 보안 취약점에 대하여 그 심각성을 평가함으로써 이에 대한 적절한 대응을 수행하도록 하기 위해 제안되었다. NVD나 ODB 등의 취약점 데이터베이스에서 CVSS에 기반한 평가 결과를 제공하고 있으며, 취약점 평가 결과로서 가장 널리 사용되고 있다. 기존의 데이터베이스에서는 시점에 의존적인 척도(Temporal Metrics)와 환경에 의존적인 척도(Environmental Metrics)가 시점 및 환경에 따라 가변적이기 때문에 기본 척도(Base Metrics)를 중심으로 평가 결과를 제시하고 있다. 본 연구의 주요 목표인 취약점 발굴 포상과 관련하여, CVSS의 척도들은 취약점의 자체의 심각성만을 평가하고 있어 본 연구가 대상으로 하는 취약점 발굴 포상을 위한 평가와는 목적의 차이가 있는 것으로 판단된다.

CWSS는 보안 약점을 위한 평가척도로서 특정 소프트웨어의 보안약점 뿐 아니라 일반적인 보안약점의 심각성을 평가하기 위하여 개발되었다. 따라서 이미 취약점이 나타나지 않은 새로 발견된 보안약점에 대한 평가도 대상으로 하고 있는 것이 특징이다. CWSS는 최근 SANS Top 25의 개발에도 사용된바 있으나, 아직 계속 갱신 중에 있으며 평가 척도에 대한 객관적 기준의 제시가 아직 완전하지 않은 것으로 판단되었다. 또한, CWSS는 일반적인 약점에 대한 평가 기준이므로, 본 연구에서 목표로 하는 새로 발견된 특정 취약점 보고의 평가와는 평가 대상에 대한 차이점이 있는 것으로 판단된다. 그러나 CWSS는 CVSS와 비교하여 좀 더 최근에 개발된 평가 척도로서 좀 더 다양한 평가 척도를 제시하고 있다는 장점을 가지고 있다.

취약점 발굴 포상제의 경우, 현실적으로 심각하다고 느끼는 시스템 및 소프트웨어에 대한 취약점에 대하여 좀 더 높은 점수를 줄 수 있도록 평가 척도가 구성되어 있다. 따라서 평가 척도가 하나의 요소만을 평가하는 것이 아니라 복합적인 성격을 가지고 있으며, 일부 척도에 대한 추가 반영 역시 평가 척도가 복합적인 요소를 가지는데 영향을 주고 있다. 이러한 방법은 실제 느끼는 심각성에 부합되는 결과를 얻는데 용이한 방법이 되나, 평가 기준의 객관성을 확보하는 데에는 상대적으로 어려움이 있는 것으로 판단된다.

제 3 절 평가 척도의 설정

1. 평가 요소의 설정

기존의 평가 방법론들을 분석한 결과, CWSS와 CVSS의 경우 포상을 위한 취약성 평가에 적절하지 않은 척도와 필요하나 누락된 척도가 존재하는 것으로 분석되었다. 기존의 취약점 포상 제도를 위한 평가 방법의 경우 척도가 복합적인 성격을 가지고 있고 기존의 CWSS 및 CVSS와 비교하여 누락된 요소가 존재하는 것으로 판단되었다. 이에 대하여 본 절에서는 일차적으로 취약점 평가를 위한 주요 고려 요소를 설정하고 이에 기반 하여 필요한 평가 척도를 도출하는 2단계의 평가방법을 사용하기로 하였다.

이를 위하여 본 연구에서는 다음과 같은 6개의 평가 요소를 설정하였다.

- o 출현도 : 해당 취약성이 얼마나 많은 시스템에서 발견될 수 있는지 여부를 평가한다. 출현도에는 해당 취약성을 가진 소프트웨어의 사용 정도나, 해당 소프트웨어에서 취약점을 가진 버전이나 설치 형태의 비중 등이 영향을 주게 된다.

- o 시스템 중요도 : 해당 취약성으로 인한 침해의 결과가 얼마나 심각한지 여부를 판정한다. 같은 취약성이라도 시스템의 종류에 따라 그 파급효과가 달라지며(예: 원자력 발전소 제어 시스템 등) 또한 해당 시스템의 용도를 고려하여 일반적인 운용 환경에서 해당 침해로 인하여 해당 조직에 미치는 피해의 정도를 예상하여 판정한다. 일반적으로 범용의 소프트웨어일 경우 이 부분의 판정이 어려우나 이에 대한 판단이 가능할 경우 이를 적극 반영할 필요가 있다.
- o 기술적 영향 : 해당 취약성으로 인해 발생할 수 있는 침해의 종류에 기반하여 해당 취약성의 심각성을 판정한다. 일반적으로 원격 코드 또는 공격 코드의 실행이 다양한 2차적인 피해를 야기하므로 가장 심각한 것으로 간주된다.
- o 공격 난이도 : 해당 취약성을 공격자가 활용하여 시스템을 침해하는 작업의 대한 기술적, 절차적 어려움 및 성공 가능성을 평가한다.
- o 대응 난이도 : 해당 취약성에 대한 대응 방법의 난이도를 평가한다.
- o 발굴 수준 : 취약점 발굴 작업의 수준을 종합적으로 평가하기 위한 요소로서 CWSS, CVSS 등의 평가방법에는 포함되지 않은 평가 요소이며 취약점 발굴의 포상과 관련하여 설정된 평가요소이다. 취약점 발굴 작업의 난이도 수준과 관련 내용을 문서화 등 발굴 작업 전반에 대한 수준을 평가한다.

2. 평가 척도의 선정

취약점 및 취약점 보고의 중요도를 평가하기 위해서는 평가 요소별로 필요한 평가 척도를 설정하여 각 요소에 대한 평가를 수행하여야 한다. 이를 위하여 기존의 평가 척도를 각 요소별로 분류하여 적절한 평가 척도를 도출하고자 하였다. 평가 척도의 설정에 있어서 주요 고려 사항은 다음과 같다.

[표 5-1] 평가 요소별 척도

평가 요소	CWSS	CVSS	취약점 발굴 포상제
출현도	출현빈도(P) 배포 범위(SC)	대상 분포(TD)	사용자 규모
시스템 중요도	비즈니스 영향(BI)	부수적 피해 잠재성 (CDP) 보안 요구 (SR) : IR, CR, AR	사용자 규모(일부)
기술적 영향	기술적 영향(TI) 권한의 획득(AP) 권한의 수준(AL)	기밀성 영향(C) 무결성 영향(I) 가용성 영향(A)	공격 방법
공격 난이도	발견 가능성(DI) 침해 가능성(EX) 접근 벡터(AV) 권한 요구도(RP) 권한 요구 수준(RL) 상호 작용 정도(LI)	접근 벡터(AV) 접근 복잡도(AC) 인증(Au) 공격 가능성(EX)	사용자 규모(일부)
대응 난이도	수정 난이도 (RE) 내부 제어의 효과(IC) 외부 제어의 효과(EC)	치료 수준(RL)	
발굴 수준			기술 난이도
	발견의 신뢰도(FC)	보고의 신뢰성(RC)	문서 완성도

o 각 평가 요소를 모두 평가할 수 있도록 평가 척도를 설정하되, 평가의 용이성을 위하여 과다한 척도 설정을 지양한다.
o 평가 척도간의 중복성 또는 의존성이 발생하지 않도록 독립적인 척도를 설정한다.
o 평가 척도별로 객관적인 기준을 제시할 수 있는 척도를 설정한다.

[표 5-1]은 평가 척도의 설정을 위하여 평가 요소별로 기존의 평가 방법론들의 평가 요소들을 분류한 것을 나타낸다.

전반적으로 CWSS가 다양한 평가 척도를 사용하고 있으며, 취약점 발굴 포상제의 기준이 가장 간략한데 이는 평가의 용이성을 위한 것으로 판단된다. 취약점 포상제의 경우에는 각 평가 척도가 여러 평가 요소를 포괄적으로 평가하고 있는 것으로 판단되며, 이는 주요 소프트웨어에 대하여 중점을 두는 결과를 가져오는 것으로 판단되었다. 각각의 평가 요소별로 평가 방법론들의 척도들을 비교하여 다음과 같이 각 요소의 평가 척도를 도출하였다.

o 출현도 : 세 평가척도 모두 취약점의 출현 빈도를 평가 기준에 포함하고 있으나, CVSS의 경우에는 환경적 요소로서 특정 환경을 고려한 영향을 평가하고 있으며, 포상제의 평가방법의 경우 다른 요소(접근 벡터, 환경에 대한 의존성, 피해의 심각성 등)를 복합적으로 평가하고 있다. CWSS는 출현빈도에 추가로 취약점을 가진 소프트웨어가 실제로 취약한 형태로 설치되는 경우의 비율을 함께 평가하고 있다. 취약점 포상 발굴제의 경우에도, 사용자 규모의 평가 시에 환경 설정이 특별한 경우의 취약점의 점수를 낮춤으로써 SC와 관련된 요소를 반영하고 있다. 이러한 요소는 평가에 모두 중요한 것으로 판단되어, 본 연구의 평가 방법에서는 소프트웨어의 파급 분포와 실제 취약한 형태로 설치, 사용되는 비율을 나타내는 대상 분포를 출현도의 평가 척도로 사용하기로 하였다.

o 시스템 중요도 : CVSS의 방법론의 경우 취약성 평가에 있어서 실제 IR, CR, AR 등의 각 보안 요소에 대한 중요도는 실제 반영이 쉽지 않으며, 대부분 환경에 의존적인 경우이기 때문에 설득력 있는 기준의 설정이 어려운 것이 사실이다. 또한, 비지니스 영향(BI)의 경우도 특정 환경에 의존적이기 때문에 일반적인 평가가 어렵다. 그러나 주로 설치되는 시스템의 일반적인 형태와, 해당 응용의 주된 사용 용도 및 취약점의 파급 피해를 고려하여, 침해로 인한 피해의 심각성을 반영하는 것은 필수적이므로 비즈니스 영향을 단일 평가기준으로 선택하여 이러한 요소를 반영하도록 하였다.

o 기술적 영향 : CVSS는 보안요소 세 분야에 대한 영향을 기준으로 기술적 영향을 평가하나, 실제로는 침해로 인하여 나타나는 2차적인 피해를 반영하지 않기 때문에 침해의 심각성을 적절히 평가하지 못하고 있다. CWSS의 경우에는 실제 문서상으로 객관적인 평가기준을 제시하고 있지 못하고 있다. 포상제의 평가기준의 경우 다양한 침해 방법을 설정하고 해당하는 침해 방법들을 합산하여 점수를 설정하고 있으나, 방법 간의 중복이 존재할 수 있다는 점이 수정 요소로 판단되며, 일반적인 형태와 개별 예시가 혼재하는 형태이다. 이에 대하여 본 연구에서는 포상제 평가방법과 같이 침해 방법의 합산으로 평가하는 방법을 취하되, 침해 방법을 선정함에 있어 CWE에서 제공하는 다양한 침해방법을 도입하여 각 평가 요소를 합산하는 방법을 사용하여 평가하고자 하였다. 침해로 인한 권한의 획득과 관련해서는 각 기존 취약성 사례에 대한 평가에 있어 큰 차이가 없는 것으로 판단되어 기술적 영향 척도만 반영하는 것으로 하였다.

o 공격 난이도 : 공격자가 침해를 성공하는데 필요한 권한, 난이도, 노력 등을 평가하는 척도로서, CWSS에서 좀 더 다양한 척도로 평가하고 있어 이를 기반으로 척도를 선정하고자 하였다. 제시된 척도 중 발견 가능성(DI)의 경우 일반적인 약점을 기준으로 해당 약점을 가진 취약점이 발견될 확률을 평가하는 것이기 때문에 이미 보고된

취약점을 평가하는 것에는 적당하지 않은 것으로 판단되어 제외하였으며, 권한 요구 수준(RL)의 경우 권한 요구도와 상호 의존성이 있으며, 취약점 평가의 경우 변별력이 크지 않을 것으로 판단되어 제외하였다. 또한 침해의 가능성에 대한 척도를 새로 설정하는데 있어 CWSS의 보고의 신뢰도 척도(FC)의 요소를 일부 반영하였다.

- o 대응 난이도 : CWSS가 더 다양한 척도를 제시하고 있으며, 두 방법론에서 제공하고 있는 네 가지 척도가 모두 상이하다. 내부 제어의 효과의 경우에는, 내부적인 코드 수정의 난이도를 평가하는 것이 포상제의 의의에 부합하지 않고, 실제 대부분의 취약점이 적절히 수정이 가능한 경우이기 때문에 척도에서 제외하였다. 또한, 척도를 간략화 하기 위하여 CVSS의 치료 수준은 CWSS의 수정의 난이도와 합하여 하나의 척도로 제시하였고, 외부 제어의 효과 역시 척도로 선택하여 2개의 척도를 사용하였다.
- o 발굴 수준 : 이 척도는 취약점의 포상과 관련된 척도이다. 본 연구에서는 기존 취약점 포상제의 평가 척도를 반영하여 발굴 난이도 척도를 추가하였고, 관련 보고서 등의 완성도를 포상의 근거 자료로 활용하기 위하여 문서 완성도를 척도로 채택하였다. 발굴 난이도의 경우 발굴 작업의 특성 상 기준 자체는 공격 난이도와 비슷할 수 있으며, 평가 척도에 대한 점수는 반대의 성격을 가진다. 공격 난이도는 이미 취약점이 알려진 상황에서의 공격의 난이도를 평가하며, 발굴 난이도는 해당 취약점이 알려지지 않은 상황에서 해당 취약점을 찾아내기 위한 난이도를 평가한다는 차이가 있다.

[표 5-2]는 최종 선정된 요소별 평가 척도를 요약하여 나타낸다.

3. 평가 척도별 의미 및 기준

본 절에서는 각 본 연구의 평가방법에서 선정한 평가척도 각각에 대한

설명과 등급별 평가 기준을 설명한다.

[표 5-2] 취약점 평가를 위한 평가 척도의 설정

평가 요소	관련 설정 척도
출현도	파급 범위, 대상 분포
시스템 중요도	피해의 심각성
기술적 영향	침해 형태
공격 난이도	접근 벡터, 권한 요구도, 상호작용 정도, 침해 가능성
대응 난이도	교정 난이도, 외부 제어의 효과
발굴 수준	발굴 난이도
	문서 완성도

1) 파급 범위

o 개요 : 이 평가 기준은 해당 보안 취약점이 발견되는 소프트웨어나 플랫폼의 보급 정도를 평가한다.

o 평가방법 : 보급률이 높고 사용자가 많은 소프트웨어나 플랫폼에서 발견되는 보안 취약점일수록 높은 값을 가진다. 좀 더 객관적인 기준을 제시하기 위하여 해당 소프트웨어의 종류와 보급도를 복합적으로 평가하여 평가하도록 하였다.

o 등급별 기준 : Widespread(W), High(H), Common(C), Limited(L), Rare(R)의 5가지 단계로 평가하며, 각 등급은 취약점을 가진 소프트웨어의 성격에 따라 다음과 같이 소프트웨어의 종류와 보급도를 기

준으로 부여된다.

종류 \ 보급도	대표적인 경우	일반적으로 알려진 경우	잘 알려지지 않은 경우
OS	W	W	H
기반시설(라우터 등)관련 운영 및 서버 SW, 시스템 소프트웨어	W	H	C
웹사이트 (포털, 은행 등) 및 웹사이트 관련 보안 프로그램	W	H	L
필수 응용 프로그램 (워드프로세서, 메신저, 플래쉬, pdf 뷰어 등) 보안 관련 프로그램	H	C	L
일반 응용 프로그램 또는 앱	C	L	L
공개 프로그램	C	L	R
개별 시스템 제어 페이지	L	L	R

부여된 등급에 대한 등급별 점수는 다음과 같다.

등급	점수
W	1
H	0.9
C	0.8
L	0.6
R	0.3

2) 대상 분포

o 개요 : 취약점을 가진 소프트웨어 중 실제로 해당 보안 취약점에 의하여 침해가 가능하도록 설치된 소프트웨어의 비율을 평가한다.

o 평가방법 : 주어진 보안 취약점이 만약 모든 배포 가능한 버전에 존재하는지, 아니면 특정한 플랫폼이나 설정에서만 발생하는지를 평가한다. 보안 취약점이 발견되는 범위가 넓고 일반적일수록 높은 점수로 평가한다.

o 등급별 기준

등급	코드	점수	평가기준
All	A	1	해당 보안 취약점이 모든 플랫폼과 설정에 존재하는 경우이다.
Moderate	M	0.9	해당 보안 취약점이 일반적인 플랫폼과 일반적으로 인스톨되는 설정에 존재하는 경우이다.
Rare	R	0.6	해당 보안 취약점이 사용빈도가 낮은 플랫폼이나 설정에 존재하는 경우이다.
Default	D	0.8	해당 보안 취약점으로 인한 침해 가능성이 해당 소프트웨어가 설치된 시스템의 특성에 따라 다양할 경우에 중간 값을 부여한다.

3) 피해의 심각성

o 개요 : 이 평가척도는 취약점을 이용한 공격이 성공하였을 때 비즈니스 혹은 임무에 미치게 되는 잠재적인 영향을 평가한다. 또한 해당 소프트웨어의 주요 용도를 판단하여, 해당 취약성으로 인한 결과가 공공의 안전 등에 심각한 영향을 주는지 여부를 복합적으로 판단한다.

o 평가방법 : 취약점을 이용한 공격으로 발생 가능한 비즈니스/임무의 운영에 대한 피해의 정도에 따라 아래 표와 같이 비즈니스 영향의 정도를 등급으로 정한다. 그러나 실제적으로 침해의 피해 정도는 특정 시스템의 사용 목적 및 운용 환경에 의존적이므로, 일반적인 우리나라에서의 평균적인 환경을 고려하여 영향도를 평가한다. 또한 해당 소프트웨어가 공공의 안전 등에 영향을 미칠 경우 해당 점수에 대한 가산점을 부여한다.

o 등급별 기준

등급	코드	점수	평가기준	비고
Critical	C	0.7	비즈니스/임무가 완전히 실패할 수 있다.	안전 및 중요 공공 서비스, 금융 등에 직접적 연관성이 있을 경우 한 등급 상향 조정한다.
High	H	0.5	비즈니스/임무의 운용이 크게 영향 받을 수 있다.	
Midium	M	0.3	비즈니스/임무의 운용이 크게 영향 받을 수 있으나 정상적인 운용에 대규모의 피해는 없다.	
Low	L	0.1	비즈니스/임무에 최소한의 영향이 있다.	
None	N	0	비즈니스/임무에 최소한의 영향이 없다.	

4) 침해 형태

o 개요 : 해당 보안 취약점을 이용한 공격으로 침해당했을 경우, 공격 성공으로 인한 기술적인 침해 형태의 다양성을 평가한다.

o 평가 방법 : CWE에서 명시하고 있는 약점에 대한 일반적인 결과(Common Consequences) 항목의 8가지 기술적 영향(Technical Impact) 내용을 사용하여 해당하는 점수를 합산한 후, 이를 기준으로 등급을 부여한다. 이때 관련성이란 해당 약점으로 인한 직접적인 결과를 의미하며, 간접적인 침해는 제외하는 것을 원칙으로 하나, 간접적인 침해의 사례가 많을 경우에는 이를 포함시킬 수 있다. 각 침해 형태에 대한 평가 점수는 전적인 침해인지 해당 계정이나 관련 파일 등의 부분적인 침해인지에 따라 구분하여 점수를 부여하며, 8가지 항목 중 Gain privileges / assume identity와 Bypass protection mechanism은 중복될 수 있는 요소이므로 하나로 병합하여 평가한다. 전체적인 평가 항목과 각 항목에 대하여 부여하는 점수는 다음과 같다.

Technical Impact 항목	전적 침해	부분적 침해	관련 없음
Modify data	2	1	0
Read data	2	1	0
DoS: unreliable execution	2	1	0
DoS: resource consumption	2	1	0
Execute unauthorized code or commands	4	2	0

Technical Impact 항목	전적 침해	부분적 침해	관련 없음
Gain privileges / assume identity, Bypass protection mechanism	2	1	0
Hide activities	2	1	0

o 등급별 기준

등급	코드	점수	평가기준
Critical	C	1	6점 이상
High	H	0.9	4점~5점
Medium	M	0.8	2점~3점
Low	L	0.7	1점
None	N	0	0점

5) 접근 벡터

o 개요 : 이 평가 척도는 취약점을 이용하여 침해를 수행하는 통로와 관련된 평가 척도로서, 원격의 접근을 통하여 침해가 가능할수록 높은 점수를 부여한다.

o 평가방법 : 제시된 취약점의 공격방법 예시를 참고하여, 침해를 위하여 주로 사용되는 접근 방법을 판단한다. 복수의 방법이 가능할 경우에는 가장 점수가 높은 등급을 선택한다. CWSS는 내부의 네트워크 접속에 대하여 Intranet, Private, Adjacent Network의 세분화된 분류를 제공하고 있으나, 평가의 용이성을 위하여 이 세 등급을 Adjacent Network로 통합하였다.

o 등급별 기준

등급	코드	점수	평가기준
Internet	I	1	일반적인 인터넷을 통하여 취약점을 침해할 수 있다.
Adjacent Network	A	0.9	방화벽 등으로 차단된 사업체의 인트라넷이나, 신뢰되는 그룹만이 접근할 수 있는 개별 네트워크 또는 물리적으로 연결된 local IP 서브넷, 블루투스, IEEE 802.11, 지역 이더넷 세그먼트 등의 인터페이스를 통한 접근이 필요하다.
Local	L	0.8	쉘 계정과 같이 운영체제에 대하여 직접 명령어를 수행하는 접근이 필요하다.
Physical	P	0.7	시스템에 대하여 USB, 키보드, CD, 마우스 등을 사용한 직접적인 물리적 접근이 있어야 침해가 가능한 경우이다.
Default	D	0.85	평가할 수 없는 경우 중간값을 부여한다.

6) 권한 요구도

o 개요 : 공격자가 취약점에 대한 공격을 수행하기 위하여 필요한 접근 권한을 평가한다.

o 평가방법 : 제시된 취약점의 공격방법 예시를 참고하여, 침해를 위하여 필요한 권한을 판단한다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	1	취약점을 가진 코드에 접근하기 위하여 아무 권한도 필요하지 않음 경우를 말한다. 일반적으로 공개되어 있는 웹 페이지를 위한 웹 응용프로그램에서 발생되는 보안 취약점이나 이메일 등을 통한 공격은 None으로 평가한다.
Guest	G	0.9	특정한 관리자의 허락을 요구하지 않고, 불특정 다수에게 허용되는 회원가입 등을 통하여 접근할 수 있는 프로그램 코드의 경우에 해당된다.
Regular User	R	0.8	특별한 관리자 권한이 없는 정규 사용자 권한을 필요로 하는 경우를 말한다.
Administrator	A	0.7	해당 소프트웨어와 운영체제 전체에 대한 접근 권한을 가진 시스템 관리자 권한이 필요한 경우를 말한다.
Default	D	0.85	해당 취약점에 대한 공격이 시스템의 환경에 따라 다양한 권한을 요구하는 경우 Default 등급으로 하며, 점수는 Guest와 Regular User의 중간값을 부여한다.

7) 상호작용 정도

o 개요 : 취약점을 공격하는데 필요한 피공격자의 협조적인 행동의 요구 수준을 평가한다.

o 평가방법 : 해당 취약점에 대한 보고서의 공격 방법 사례를 참조하거나, CAPEC의 공격 패턴 등을 참고하여 해당 공격이 성공하기 위하여 희생자가 수행해야 하는 협조적인 동작의 수준을 평가한다. 시

스템의 환경에 따라 여러 기준에 모두 해당하는 경우 해당 값들의 중간(median) 값을 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
Automated	A	1	희생자측의 협조적인 행동이 필요 없다.
Limited/Typical	L	0.9	희생자의 일반적인 행동(이메일 열람, 웹 페이지 접근)이 동반되어야 침해가 가능하다.
Moderate	M	0.8	희생자가 경고 메시지를 무시하는 것과 같은 어느 정도 위험할 수 있는 작업을 수행하여야 해당 보안약점에 대한 공격이 이루어진다.
High	H	0.7	희생자가 잘못된 행동을 하도록 희생자에 대한 직접적인 접근을 포함한 복잡한 사회적 작업을 수행하여야 한다.

8) 침해 가능성

o 개요 : 보안 취약점을 가진 시스템에 대하여 필요한 공격에 필요한 권한과 접근 및 희생자의 협조적인 행동을 획득한 공격자가 실제로 침해에 성공하여 피해를 입힐 가능성을 기법의 난이도 및 취약점의 성격, 실제적인 피해의 발생 가능성 등을 반영하여 평가한다.

o 평가방법 : 취약점 보고서의 공격 예시를 반영하여, 공격의 난이도와 성공 가능성을 판단한다. 시스템의 특성에 따라 다양하게 분포되어 있을 경우 Default 값을 부여한다. 단, 본 평가는 취약점 자체 및

공격 시도 과정의 기술적 난이도의 특성에만 기반하며, 특정 소프트웨어 설정에 대한 의존성, 접근 권한의 획득, 접근 벡터, 사용자와의 상호작용 요구 정도 등의 특성은 무시한다.

o 등급별 기준

등급	코드	점수	평가기준
High	H	1	해당하는 약점에 대한 표준적인 공격 기법이 존재하거나 해당 소프트웨어의 취약점에 해당하는 공격 방법이 알려져 있으며, 다른 요소(희생자 협조 등)가 동반될 경우 보안 침해의 발생 가능성이 높다.
Medium	M	0.9	해당 소프트웨어의 취약점에 해당하는 공격 방법이 개발이 실제적으로 가능하며, 다른 요소(희생자 협조 등)가 동반될 경우 보안 침해의 발생 가능성이 높다.
Low	L	0.8	해당 소프트웨어의 취약점에 해당하는 공격 방법이 개발이 실제적으로 어렵거나, 다른 요소(희생자 협조 등)가 동반된다 하여도 보안 침해의 발생 가능성이 낮은 경우이다.
Very Low	VL	0.7	해당 소프트웨어의 취약점에 해당하는 공격 방법이 개발이 실제적으로 어려우며, 다른 요소(희생자 협조 등)가 동반된다 하여도 보안 침해의 발생 가능성이 낮은 경우이다.
None	N	0	해당 취약점에 대한 공격으로 인한 보안 침해가 발생할 가능성이 없을 경우이다.

9) 교정 난이도

o 개요 : 취약점을 제거하는데 필요한 난이도를 평가하며, 이는 코드 수정의 난이도와 함께 공식적인 패치의 존재 여부 및 패치 적용의 난이도도 함께 평가한다.

o 평가방법 : 해당 취약점에 대한 보고서의 공격 방법 사례와 관련 취약점 방어 기술의 동향을 참고하여, 취약점 방어의 난이도를 아래 기준에 따라 평가한다. 소스코드의 미 확보와 취약점 특성으로 인하여 난이도를 평가할 수 없을 경우에는 중간값을 점수로 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
Extensive	E	1	공식적인 패치는 존재하지 않으며, 교정을 위하여 설계와 전체 시스템 구조의 수정과 같은 전체적인 수정이 필요하여 상당한 작업과 시간이 필요하다.
Moderate	M	0.9	소스 파일의 복수개의 모듈 수정과 같은 중간 정도의 수정이 필요하며, 설계와 구조에 대한 수정은 필요 없다. 또는, 공식적인 패치가 존재하나, 해당 패치를 적용하기 위해서는 관련 시스템이 일정기간 중단되어야 하는 등 전체 서비스에 지장을 초래할 수 있다.
Limited	L	0.8	한 모듈 내의 적은 수의 라인의 코드에 대한 수정을 요구하며, 일정한 수준의 노력과 시간이 필요하다. 또는 공식적인 패치가 존재하며, 관련 시스템 서비스의 운영에 대한 어려움 없이 패치의 적용이 가능하다.

등급	코드	점수	평가기준
Default	D	0.9	소스코드의 미확보와 취약점 특성 등으로 인하여 필요한 난이도를 평가할 수 없을 경우 중간값(Modearte)과 동일한 점수를 부여한다.

10) 외부 제어의 효과

o 개요 : 소프트웨어 외부의 추가적인 시스템을 통하여 해당 취약점을 제어하는 방법의 효과를 평가한다.

o 평가방법 : 아래 등급별 기준에 따라 외부 제어의 효과를 평가한다. 제어의 효과가 높을수록 취약점의 심각성 점수는 낮게 평가된다. 여러 등급에 해당할 때에는 심각성이 가장 높은 경우를 선택한다.

o 등급별 기준

등급	코드	점수	평가기준
None	N	1	외부적으로 제어할 수 있는 방법이 없다.
Limited	L	0.9	간단한 방법이나, 부분적인 제한만이 가능하며, 초보적인 공격에 대해서만 방어가 가능하다.
Moderate	M	0.8	일반적으로 사용되는 방어 방법이 존재하나, 지식을 가진 공격자에 의하여 필요한 노력이 동반될 경우 침해될 수 있다.

등급	코드	점수	평가기준
Indirect	I	0.7	해당 침해를 전적으로 방어하지는 못하나, 공격의 피해를 줄이는 방법이 존재한다. 예를 들어 ASLR 방법은 잘못된 코드의 수행은 막을 수 있으나 프로그램의 중단되는 결과는 감수하여야 한다.
Best Available	B	0.6	적용 가능한 방어 방법이 존재하나, 숙련된 공격자가 다른 취약점을 함께 사용하여 공격할 경우 침해가 발생할 수 있는 가능성이 존재한다.
Complete	C	0.4	약점에 대하여 전적으로 효과적인 방법이 존재한다. 예를 들어 sandbox 방법을 통하여 파일 접근을 제어할 수 있다.
Default	D	0	취약점에 대하여 다양한 후보 대응방법이 존재하나 그 효과가 명확하지 않을 경우에 중간값을 부여한다.

11) 발굴 난이도

o 개요 : 취약점 발굴 포상을 위하여 채택한 특징적인 척도로서 취약점을 발굴에 필요한 노력 및 난이도를 직접적으로 평가한다. 발굴의 난이도는 공격의 난이도와 대칭적인 관계로서, 이미 알려져 있는 취약점일 경우에는 발굴의 난이도가 공격 난이도에 연계된다고 할 수 있다. 일반적으로 발굴 난이도가 높을수록 공격 난이도도 높아지는 경향이 있으며, 부여되는 점수는 반대의 성격을 가지게 된다.

o 평가방법 : 기존에 알려지지 않은 방식의 취약점이고, 발굴의 난이도가 높을수록 높은 점수를 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
Very High	VH	1	기존에 알려지지 않은 방식의 취약점으로 발굴 난이도 높음
High	H	0.9	기존에 알려지지 않은 방식의 취약점이나 발굴 난이도 낮음
Midium	M	0.7	기존에 알려진 방식의 취약점으로 이를 활용하기 위한 발굴 난이도 높음
Low	L	0.6	기존에 알려진 방식의 취약점으로 발굴 난이도 낮음

12) 문서 완성도

o 개요 : 해당 보안 취약점에 대한 보고서의 완성도와 신뢰성을 평가한다.

o 평가방법 : 보고된 보안 취약점의 진위 여부와 보고의 충실도를 평가한다. 실제로 보안 취약점이 공격자가 이용할 수 있는 형태로 존재하며, 동작 환경에 대한 설명이 구체적일수록 높은 점수를 부여한다.

o 등급별 기준

등급	코드	점수	평가기준
High	H	1	해당 보안 취약점에 대한 침해 방법이 재현 할 수 있는 형태로 명확히 제시되어 있으며, 동작 환경 등에 대한 설명이 존재하는 경우이다.

등급	코드	점수	평가기준
Medium	M	0.8	해당 보안 취약점에 대한 침해 방법이 재현 할 수 있는 형태로 명확히 제시되어 있으나, 동작 환경 등에 대한 설명이 존재하지 하는 경우이다.
Low	L	0.6	해당 보안 취약점에 대한 침해 방법이 일정 수준 설명되어 있으며, 동작 환경 등에 대한 설명이 존재하는 경우이다.
Very Low	VL	0.4	취약점에 대한 침해 방법의 설명이 미흡하거나, 동작환경 등에 대한 설명의 부재로 인하여 침해의 재현이 어려울 것으로 판단되는 경우이다.

제 4 절 중요도 점수의 산정

본 절에서는 중요도의 점수 산정을 위한 공식을 제시한다. 전체 중요도 점수는 신규 취약점 발굴 포상을 위한 점수인 취약점 발굴 점수와 보안 취약점 DB 구축 등을 위해서 사용될 수 있는 취약점 DB 점수의 두 가지 산출 방법을 제시한다.

본 연구에서 제시한 12개의 취약점 평가 척도는 취약점 포상제의 평가와 일반적인 취약점 중요도 평가 모두에 사용될 수 있는 취약점 평가의 전반적인 부분을 모두 포함하고자 하였다. 따라서 취약점 포상제와 일반적인 취약점 데이터베이스 구축의 두 가지 목적에 따라서 적절한 평가요소를 선택적으로 사용하는 것이 바람직한 것으로 판단된다.

[표 5-3]은 본 연구에서 설정된 평가요소에 대하여 신규 취약점 발굴 포상과 취약점 DB 구축시의 중요도 점수 부여의 목적에 따른 적용 평가요소를 나타낸 것이다. 취약점 발굴 점수의 경우에는 해당 취약점의 대응은 시스템 개발자나 사용자가 수행하여야 하는 부분이므로 해당 항목

[표 5-3] 목적에 따른 평가 요소의 반영

평가 요소	관련 설정 척도	취약점 발굴 포상	취약점 DB 구축
출현도	파급 범위 대상 분포	O	O
시스템 중요도	피해의 심각성	O	O
기술적 영향	침해 형태	O	O
공격 난이도	접근 벡터 권한 요구도, 상호작용 정도, 침해 가능성	O	O
대응 난이도	교정 난이도, 외부 제어의 효과	X	O
발굴 수준	발굴 난이도 문서 완성도	O	X

을 평가에서 제외하였으며 취약점 DB 점수는 취약점 발굴 수준 관련 척도의 경우 발굴자의 보고의 신뢰성 및 노력을 평가하기 위한 것이므로 해당 요소를 평가에서 제외하였다.

이러한 점을 반영하여 목적에 따라 설정한 목적별 중요도 점수는 다음과 같다.

o 취약점 발굴 점수 = 취약점 점수 * 8 + 발굴 수준 점수 * 2
o 취약점 DB 점수 = 취약점 점수 * 8 + 대응 난이도 점수 * 2

위에서 제시하는 바와 같이 취약점 발굴 점수의 경우 발굴의 수준을 점수화한 발굴 수준 점수가 반영되며, 취약점 DB 점수의 경우에는 대응 난이도 점수가 대신하여 포함된다. 취약점 점수와 발굴 수준 점수, 대응

난이도 점수는 0~1의 범위를 가지며, 총점은 10점 만점으로 계산된다.

취약점 점수, 발굴 수준 점수, 대응 난이도 점수의 산출 방법은 다음과 같다.

o 취약점 점수 = 영향도 점수 * 출현도 점수 * 공격 난이도 점수
  - 영향도 점수 = 침해 형태 + (1-침해 형태) * 피해의 심각성 (침해 형태가 0이 아닌 경우)
    0 (침해 형태가 0인 경우)
  - 출현도 점수 = 파급 범위 * 0.8 + 대상 분포 * 0.2
  - 공격 난이도 점수 = (접근 벡터 + 권한 요구도 + 상호작용 정도) * 침해 가능성 / 3
o 발굴 수준 점수 = (발굴 난이도 + 문서 완성도) / 2
o 대응 난이도 점수 = (교정 난이도 + 외부 제어의 효과) / 2

영향도 점수에 있어서 기술적 영향 척도의 점수가 기본적으로 사용되며, 피해의 심각성은 부수적으로 반영되어 기술적 영향이 다양하지 않더라도 피해의 심각성이 크면 점수가 1에 가까워진다. 출현도에 있어서는 기존 취약점 보상제와 마찬가지로 파급 범위에 중점을 두어 점수를 부여하게 된다. 공격 난이도의 경우에는 공격의 방해 및 필요 요소와 관련된 세 가지 척도의 산술 평균에 해당 공격으로 인한 침해의 발생 가능성을 곱하여 계산함으로써, 공격으로 인한 실제 침해가 없을 경우에 이를 전체적으로 반영할 수 있도록 하였다. 또한, 발굴 수준, 대응 난이도 점수는 관련 척도의 평균을 사용하도록 하였다.

참고 문헌

[1] CWE - Common Weakness Scoring System (CWSS), http://cwe.mitre.org/cwss/

[2] A Complete Guide to the Common Vulnerability Scoring System Version 2.0, http://www.first.org/cvss/cvss-guide

[3] 안준선, 방지호, 이은영, “소프트웨어 보안약점의 중요도에 대한 정량 평가 기준 연구”, 정보보호학회논문지, 19권6호, pp.1407-1417, 2012년.

제 6 장 결론

본 연구에서는 SW 취약점 발굴 포상 및 SW 취약점 DB 구축 사업에 활용될 수 있는 보안 취약점 정량 평가 방법의 개발을 목표로 한다. 이를 위하여 다음과 같은 연구를 계획에 따라 진행하였다.

- o 국·내외 보안 취약점 평가체계 및 적용 관련 동향 조사 : 국외 취약점 및 보안약점 평가 방법인 CWSS와 CVSS에 대한 조사를 수행하고, 시범 평가를 위한 기준 수립 등의 작업을 수행하였다. 또한 관련 취약점 DB인 OSDVB, NVD 등에 대한 조사를 수행하여 해당 DB에서의 보안 취약점 적용 사례를 조사하였다. 아울러 국내외의 취약점 포상 사례를 조사하였고, 주요 민간업체의 적용 사례 및 관련 표준화 사례를 조사하였다. 또한 인터넷진흥원의 추가적인 요청에 의하여 중국에서 구축되고 있는 CNVD 보안 취약점 데이터베이스 구축사례에 대하여 조사를 수행하였다.
- o 소프트웨어 대상 신규 보안 취약점 평가 방법 연구 : 취약점을 평가하는데 있어서 해당 보안 취약점의 파급도 및 위험도를 반영한 취약점 평가 방법을 개발하기 위하여 보안 취약점의 심각성에 대한 6개 평가 요소를 설정하고 관련 12개 평가 척도를 제시하였다. 또한 이러한 평가 척도에 기반하여 취약점 발굴 포상과 취약점 DB 구축에 사용하기 위한 정량적인 중요도 산출 공식을 각각 제시하였다.
- o 보안 취약점 평가 체계 시범 적용 : CWSS와 CVSS 평가 척도를 활용하여, KISA에서 제공한 40개 보안 취약점 발굴 사례에 대한 시범 평가를 수행하였다. 또한 KISA에서 새로 개발된 취약점 평가 방법에 기반하여 2가지 목적을 위한 중요도 정량 시범평가를 수행하였다.

[표 6-1] 추진일정 대비 진척도

과 제 내 용	추 진 일 정 (월별)					
	4	5	6	7	8	진척도
▪ 국·내외 보안 취약점 평가체계 및 적용 관련 동향 조사						
- 미 FIRST의 CVSS 분석	■	■	■			100%
- 미 MITRE의 CWSS 분석	■	■	■			100%
- 미 NVD 및 OSVDB 등 보안 취약점 DB 분석	■	■	■	■		100%
- 보안 취약점 관련 국제 표준화 추진동향 분석			■	■		100%
- 주요 민간 업체의 보안 취약점 평가방법 분석			■	■		100%
- 취약점 포상 사례를 통한 보안 취약점 평가방법 적용사례 분석			■	■		100%
▪ 소프트웨어 대상 신규 보안 취약점 평가 방법 연구						
- 국내 환경을 고려한 보안 취약점 파급도 및 위험도 평가 연구		■	■	■		100%
- 소프트웨어 대상 신규 보안 취약점 평가방법 개발			■	■		100%
▪ 보안 취약점 평가 체계 시범 적용						
- 국내 SW 보안 취약점 대상 CVSS 및 CWSS 시범 적용		■	■	■		100%
- 연구 개발된 보안 취약점 평가방법 시범 적용				■	■	100%
▪ 보고서 작성 및 산출물 제출						
- 중간보고서 작성			■			100%
- 최종보고서 작성					■	100%
- 연구산출물 제출					■	100%

전체적으로 추진 일정에 따라 연구를 진행하였고, 연구제안서의 내용을 충실히 수행하였다. 연구를 수행하는 동안, 1차 시범평가, 평가척도 도출, 평가식 도출, 시범평가 완료의 각각의 단계에서 인터넷진흥원과의 4차례의 공식적인 회의를 통하여 수시로 연구 결과를 조율하였다.

제안된 보안 취약점 평가방법은 다음과 같은 장점을 가진다.

- o 점수를 부여함에 있어서 기존의 보안 취약점 및 보안약점 평가방법에서 사용하는 평가방법의 척도 및 기존 인터넷진흥원에서 이미 사용하고 있는 포상제 평가 척도를 모두 고려하여, 가장 적합한 척도를 선택하여 사용하였다.
- o 평가척도를 구성함에 있어 6개 필수 평가범주를 설정하고 이에 맞추어 척도를 선택함으로써 균형있는 분석이 될 수 있도록 하였다.
- o 국내 실정에 맞는 적절한 평가 기준을 수립하기 위하여 국내의 파급도를 반영할 수 있도록 관련 척도를 적절히 설계하였다.
- o 평가 공식의 설정에 있어서, 보안 취약점의 영향도, 출현도, 공격난이도의 취약점 특성과 발굴의 수준 및 대응 난이도를 독립적으로 평가하고, 그 결과를 기반으로 목적에 맞는 평가 방법을 도출할 수 있도록 하였다. 이를 통하여 한 가지 특성에 대한 중복되는 점수 반영 가능성을 최소화하였다.

제안된 평가방법을 사용하여 인터넷진흥원에서 제시한 국내 보안 취약점 사례 40건에 대한 시범평가를 수행하고, 그 결과를 인터넷진흥원과 공동으로 점검하여 평가 척도 및 공식을 재수정하는 과정을 거침으로써 설득력 있는 평가가 이루어질 수 있는 보안 취약점 평가 체계를 도출하였다.

제시된 취약점 평가체계는 모든 척도에 대하여 객관적 기준을 적절한 체계에 의하여 제시하였고, 중요도 산출 공식의 도출에 있어서도 논리적인 근거에 기반한 체계를 제시였기 때문에, 설득력을 확보하면서도 향후 추가적인 환경의 변화 또는 요구조건의 변화에도 적절히 대처하여 갱신하는 것도 용이할 것으로 판단된다.

개발된 보안 취약점 평가체계는 현재 인터넷진흥원에서 진행하고 있는 보안 취약점 발굴 포상제의 포상 근거로 바로 활용이 가능할 것으로 판

단된다. 또한 차후 보안 취약점에 대한 종합적인 DB 구축이 추진될 경우 주요 제공 정보인 보안 취약점 중요도 점수 및 근거를 객관적으로 제공하는데 사용할 수 있다.

소프트웨어 보안 취약점 평가체계 연구

인 쇄 : 2013 년 8 월
발 행 : 2013 년 8 월

발행인 : 이 기 주
발행처 : 한국인터넷진흥원(KISA, Korea Internet&Security Agency)
서울시 송파구 중대로 109 대동빌딩
Tel: (02) 405-4118
인쇄처 : 카피랜드
Tel: (02) 3159-8114

<비매품>