JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 11, pp. 283-297, November 2026
https://doi.org/10.9708/jksci.2026.31.11.283

A Study on Listing Time Lags between CISA KEV and VulnCheck KEV and Design Criteria for a Korean KEV

Seung Han Yoon*, Ah Reum Kang**

*Student, Dept. of CyberSecurity, Pai Chai University, Daejeon, Korea
**Professor, Dept. of CyberSecurity, Pai Chai University, Daejeon, Korea

[Abstract]

Known Exploited Vulnerability (KEV) catalogs are a key basis for vulnerability prioritization, yet evidence on how quickly and broadly public and private catalogs capture exploited vulnerabilities is limited. Integrating 1,726 CISA KEV entries, 5,361 VulnCheck KEV entries, and NVD, EPSS, and GitHub PoC data, we analyzed the lag from NVD publication to KEV listing. All CISA KEV entries were contained in VulnCheck KEV, but within the common observation period (Nov. 3, 2021–Sep. 25, 2026), CISA KEV covered only 28.9% of VulnCheck KEV entries. A naive comparison overstated VulnCheck's lead at a mean of 526.6 days, whereas the window-aligned median lead was only 2 days. The 30-day probability of CISA adopting a VulnCheck KEV entry was 23.9%, and at listing, 64.5% of KEV entries had no public PoC and 26.2% had an EPSS score below 0.1. As these lags reflect differences in purpose and verification rather than performance, we propose a four-stage complementary model that uses VulnCheck KEV as an early warning and CISA KEV as a verified remediation baseline, together with seven design criteria and data items for a Korean KEV linked to the national CVD/VDP pilot.

▸ **Key words**: CISA KEV, VulnCheck KEV, Time-to-Listing, CVD / VDP, Vulnerability Prioritization

[요 약]

알려진 악용 취약점(KEV) 목록은 조치 우선순위의 핵심 근거이나, 공공·민간 목록의 악용 취약점 포착 속도와 범위에 대한 실증 근거는 부족하다. CISA KEV 1,726건, VulnCheck KEV 5,361건과 NVD·EPSS·GitHub PoC 자료를 통합하여 NVD 게시–KEV 등재 시차를 분석한 결과, CISA KEV는 모두 VulnCheck KEV에 포함되었으나 공통 관측 기간(2021-11-03~2026-09-25)에는 VulnCheck KEV의 28.9%만 포함하였다. 단순 비교 시 선행일수는 평균 526.6일로 과대 추정되었으나, 관측 기간 정합화 후 중앙값은 2일이었다. VulnCheck KEV의 30일 내 CISA 편입 확률은 23.9%였고, 등재 시점에 KEV의 64.5%는 공개 PoC가 없었으며 26.2%는 EPSS가 0.1 미만이었다. 이 시차는 우열이 아닌 목적과 검증 절차의 차이이므로, VulnCheck KEV(조기 경보)와 CISA KEV(조치 기준)를 결합한 4단계 상호보완적 운영 방안과 국내 CVD/VDP 시범사업과 연계한 국내형 KEV의 7대 설계 기준 및 수집 항목을 제안하였다.

▸ **주제어**: CISA KEV, VulnCheck KEV, 등재 시차, 취약점 신고·조치·공개 제도, 취약점 우선순위

• First Author: Seung Han Yoon, Corresponding Author: Ah Reum Kang
*Seung Han Yoon (nuricaps@naver.com), Dept. of CyberSecurity, Pai Chai University
**Ah Reum Kang (armk@pcu.ac.kr), Dept. of CyberSecurity, Pai Chai University
• Received: 2026. 10. 06, Revised: 2026. 10. 21, Accepted: 2026. 11. 02.

Copyright © 2026 The Korea Society of Computer and Information
http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945
www.kci.go.kr

I. Introduction

1.1 Research Background and Purpose

매년 공개되는 공통 취약점 식별자(CVE: Common Vulnerabilities and Exposures)의 수는 빠르게 늘어나고 있으나, 조직이 가용한 인력과 시간 안에 모든 취약점을 조치하는 것은 사실상 불가능하다. 이에 따라 취약점 관리의 핵심 과제는 “무엇을 먼저 조치할 것인가”라는 우선순위 결정으로 옮겨 왔다. 전통적으로 널리 쓰여 온 CVSS(Common Vulnerability Scoring System)는 취약점의 기술적 심각도를 표현하지만 실제 악용 여부를 반영하지 못한다는 한계가 지적되어 왔고[8], 이를 보완하기 위해 악용 확률을 예측하는 EPSS(Exploit Prediction Scoring System)[5][6]와 실제 악용 증거를 목록화한 알려진 악용 취약점(KEV: Known Exploited Vulnerabilities) 카탈로그가 등장하였다.

미국 사이버보안·인프라보안청(CISA)은 2021년 11월 3일 구속력 있는 운영 지침 BOD 22-01(Binding Operational Directive 22-01)과 함께 KEV 카탈로그를 공개하였다[1][2]. CISA KEV는 실제 악용 증거가 확인되고 명확한 조치 방법이 존재하는 CVE만 등재하며, 연방 민간 기관에 조치 기한(Due Date)을 부과한다. 2026년 6월 10일에는 BOD 22-01을 갱신하는 BOD 26-04가 발령되어, KEV 등재 여부를 자산 노출, 공격 자동화 가능성, 악용 후 기술적 영향과 함께 조치 우선순위를 정하는 네 가지 기준의 하나로 재정립하였다[3]. 한편 민간 위협 인텔리전스 기업 VulnCheck는 CISA보다 넓은 수집 기준을 적용한 VulnCheck KEV를 운영하고 있다[4].

두 목록은 목적과 등재 기준이 다르다. CISA KEV는 악용 증거와 명확한 조치 방법이 확인된 뒤에 등재되어 연방 기관의 조치 의무로 이어지는 ‘방어 조치 목록’인 반면, VulnCheck KEV는 공개된 악용 증거를 넓고 빠르게 수집하여 알리는 ‘조기 경보 목록’에 가깝다. 따라서 두 목록 사이의 등재 시차는 어느 한쪽의 지연이라기보다 검증과 조치 방법 확인에 필요한 시간이 반영된 구조적 차이로 이해해야 한다. 실무에서 중요한 것은 어느 목록이 더 빠른가가 아니라 경보 단계와 조치 단계를 어떻게 연결하여 두 목록을 함께 활용할 것인가이며, 이를 설계하려면 두 목록의 시차와 범위 차이에 대한 정량적 근거가 필요하다. 그러나 기존 연구는 주로 CISA KEV 단일 목록의 구성이나 EPSS와의 결합 효과를 다루었고[11][12][16], 두 목록의 등재 시점을 동일 CVE 단위로 짝지어 비교한 분석은 2024~2025년 표본을 다룬 보안업계 보고서[30] 정도에 그치며, 학술 연구로는 드물다. 특히 CISA KEV 출범 이전의 VulnCheck 등재일을 그대로 비교에 포함하면 “VulnCheck가 수년 앞선다”는 착시가 발생할 수 있으나, 이 관측 기간 불일치 문제를 다룬 연구는 확인되지 않았다.

1.2 Policy Context in Korea

국내에서는 이 문제가 정책적으로 더욱 시급하다. 한국인터넷진흥원(KISA)에 신고된 침해사고는 2024년 1,887건에서 2025년 2,383건으로 약 26.3% 증가하였고, 같은 해 주요 통신사와 대형 전자상거래 기업의 대형 침해사고, 행정망 해킹이 연쇄적으로 발생하였다[22]. 사고가 발생한 기업들이 모두 정보보호 관리체계(ISMS: Information Security Management System) 인증을 보유하고 있었다는 점은, 연 1회 체크리스트 중심의 인증·점검 체계가 실시간으로 진화하는 공격에 대한 실제 방어 역량을 보장하지 못한다는 한계를 드러냈다[22].

이에 국가인공지능전략위원회는 2026년 2월 “보안 취약점 신고·조치·공개 제도(CVD/VDP) 도입 로드맵”을 발표하고, 2026년 하반기 시범사업, 2027년 참여 확대와 법제화를 거쳐 공공은 의무화, 민간은 참여를 유도하는 방향을 제시하였다[22]. 이는 미국 CISA의 BOD 20-01[23]과 EU의 NIS2 지침[24], 사이버복원력법(CRA: Cyber Resilience Act)[25]을 참고한 것이다. 그러나 현행 취약점 신고포상제는 2025년 한 해 2,525건의 신고를 접수하고도 취약점이 공개된 사례가 3건에 그쳐, 신고된 취약점이 조치·공개로 이어지는 연결 고리가 약한 상태이다[22].

CVD(Coordinated Vulnerability Disclosure)/VDP(Vulnerability Disclosure Policy)가 “취약점을 찾아 알리는” 단계라면, KEV(Known Exploited Vulnerabilities)는 그중 “실제로 악용되고 있어 먼저 막아야 하는” 취약점을 가려내는 다음 단계이다. 로드맵은 신고·조치·공개 체계와 90일 수준의 조치 기간을 제안하고 있으나, 국내에는 실제 악용 증거에 기반한 우선순위 목록과 조치 기한 체계가 아직 없다. 따라서 해외 KEV 목록이 얼마나 빠르고 넓게 악용 취약점을 포착하는지를 실증적으로 파악하는 것은 국내 제도 설계의 기초 자료가 된다. 특히 2026년 5월 발표된 시범사업에는 민간기업 7곳과 공공기관 8곳 등 15개 기관이 참여하여 6월부터 5개월간 실제 운영 망을 대상으로 취약점 탐색이 이루어지며, 발견된 취약점과 조치 결과는 연말에 공개될 예정이다[29]. 이는 국내에서 신고·조치·공개 전 과정이 처음으로 기록되는 기회이므로, 이 단계에서 국내형 KEV 운영에 필요한 날짜 정보와 악용 증거를 함께 수집하도록 설계해야 사후에 체계적인 평가가 가

www.kci.go.kr

능하다[22].

본 연구의 목적은 CISA KEV 공식 카탈로그, VulnCheck KEV 전체 스냅샷, NVD·EPSS·PoC 관측 자료를 통합하여 NVD(National Vulnerability Database) 게시와 KEV 등재 간 시차, 두 목록 간 선행성, 관측 기간 정합 여부에 따른 추정치의 차이, 그리고 등재 시점에 공개 PoC(Proof of Concept)와 EPSS 같은 예측 신호가 얼마나 존재하는지를 실증적으로 규명하는 데 있다. 나아가 이 결과를 두 목록의 상호보완적 운영 방안과, 국내 CVD/VDP 시범사업의 신고·조치·공개 자료와 연계할 수 있는 국내형 KEV 설계 기준과 수집 데이터 항목으로 구체화하고자 한다.

1.3 Research Questions

본 연구는 다음 여섯 가지 연구질문(RQ)을 설정하였다. 각 질문은 국내형 KEV(K-KEV)를 설계할 때 반드시 답해야 하는 실무적 질문에 대응하도록 구성하였으며, 질문마다 그 필요성과 연결되는 설계 기준(C1~C7, Table 13)을 함께 제시한다.

RQ1. CVE가 NVD에 게시된 후 CISA KEV에 등재되기까지 얼마나 걸리며, 그 분포는 어떠한가? KEV를 기준으로 조치 우선순위를 정하는 조직에게 이 기간은 악용이 진행 중인데도 우선 조치 대상으로 인식하지 못하는 노출 기간이므로, K-KEV의 등재 목표 기간(C2)을 정하는 기준선이 된다.

RQ2. 공통 관측 기간에서 CISA KEV와 VulnCheck KEV는 어느 범위에서 겹치고 어느 범위에서 다른가? 포함 범위의 차이는 공공 목록 하나만 볼 때 놓치는 악용 취약점의 규모를 뜻하므로, K-KEV가 어떤 출처를 결합해야 하는지(C3)를 판단하는 근거가 된다.

RQ3. 관측 기간을 정합화했을 때 VulnCheck KEV는 CISA KEV보다 실제로 얼마나 먼저 등재하는가? 선행일수는 민간 목록을 함께 모니터링할 때 얻는 추가 대응 시간이므로, 두 목록의 상호보완적 운영과 해외 KEV 후보의 검토 기한(C4)을 정하는 근거가 된다.

RQ4. 관측 기간을 정합화하지 않은 단순 비교는 선행효과를 얼마나 과대 추정하며, 기준일을 바꾸어도 결론이 유지되는가? 측정 방법에 따라 추정치가 크게 달라지면 정책 판단도 왜곡되므로, K-KEV 성과지표의 측정 방식(C7)을 정하는 근거가 된다.

RQ5. NVD 게시 이전 등재(음수 시차)는 얼마나 발생하며, CVSS·EPSS·PoC·랜섬웨어 악용 여부는 등재 시차와 어떤 관계가 있는가? 이는 NVD 게시나 CVSS 점수를 기다리지 않고 등재해야 하는 상황이 얼마나 있는지를 보여주므로, 등재 근거(C1)와 등재 속도(C2)를 정하는 근거가 된다.

RQ6. KEV 등재 시점에 공개 PoC와 EPSS 같은 예측 신호는 얼마나 존재하며, 이는 두 목록의 상호보완적 운영과 국내형 KEV 설계에 어떤 시사점을 주는가? 예측 신호의 존재 여부는 PoC나 EPSS를 등재 요건으로 삼을 수 있는지와, 등재 후 공격 코드 확산에 대비한 조치 기한·공개 방식(C1, C5, C6)을 정하는 근거가 된다.

1.4 Research Approach and Paper Structure

본 연구는 두 목록을 속도의 우열로 평가하기보다, 목적과 등재 기준이 서로 다른 두 목록이 어떻게 역할을 나누어 함께 활용될 수 있는지를 밝히는 데 초점을 둔다. 이를 위해 다음 네 가지를 수행한다. 첫째, 공식 원자료를 이용하여 두 목록의 포함 관계와 공통 관측 기간 기준의 포함 범위를 확인한다. 둘째, 관측 기간 불일치가 두 목록 간 선행 효과 추정에 미치는 편향을 정량화하고, 기준일을 바꾸어 결과의 안정성을 점검한다. 셋째, 중도절단(censoring)을 고려한 생존분석으로 VulnCheck KEV 항목이 CISA KEV에 편입되는 시간 구조를 분석하고, 등재 시점의 PoC·EPSS 신호를 함께 검토한다. 넷째, 이 결과를 바탕으로 민간 KEV의 조기 경보 기능과 공공 KEV의 조치 기준 기능을 결합하는 상호보완적 운영 방안을 제시하고, 이를 국가인공지능전략위원회의 CVD/VDP 도입 로드맵[22] 및 2026년 6월 시작된 시범사업과 연계한 국내형 KEV 설계 기준과 수집 데이터 항목으로 구체화한다.

제2장에서는 관련 연구를 검토하고, 제3장에서는 데이터와 분석 방법을 설명한다. 제4장에서는 연구 질문별 분석 결과와 이를 종합한 시사점을 제시하며, 제5장에서는 결과의 의미와 기존 연구와의 비교, 시사점, 두 목록의 상호보완적 운영 방안, 국내형 KEV 설계 기준, 연구의 한계를 논의한다. 제6장에서 결론을 맺는다.

본 연구는 Table 1과 같이 2026년 2월부터 9월까지 네 단계로 수행하였다. 2~3월에는 취약점 우선순위와 KEV에 관한 선행연구, 국내외 CVD/VDP 및 KEV 정책을 검토하였다. 4~5월에는 여러 출처의 자료를 CVE 단위로 통합하고 통계를 자동 산출하는 분석 도구를 설계·구현하였다. 6~9월에는 이 도구로 CISA KEV, VulnCheck KEV, NVD, EPSS, GitHub PoC 자료를 수집하였으며, 수집 절차를 반복 점검한 뒤 2026년 9월 25~27일의 최종 스냅샷을 분석 자료로 확정하였다. 8~9월에는 관측 기간을 정합화한 통계 분석과 국내형 KEV 설계 기준 도출을 수행하였다.

www.kci.go.kr

Table 1. Research Flow

Stage	Month	Contents
Literature & Policy Review	Feb ~ Mar	• Previous Studies • KEV & CVD/VDP Policy Analysis
Tool Development	Apr ~ May	• Tool Design & Implementation • Automated Statistics Module
Data Collection	Jun ~ Sep	• CISA / VulnCheck KEV, NVD, EPSS, PoC • Final Snapshot (Sep 2026)
Analysis	Aug ~ Sep	• Period-Aligned Statistics • K-KEV Design Criteria

II. Related Research

2.1 Exploitation Prediction and Vulnerability Prioritization

Allodi와 Massacci[8]는 사례-대조 연구(Case-Control Study) 설계를 도입하여 실제 악용된 취약점(사례군)과 악용되지 않은 취약점(대조군)을 비교함으로써 CVSS 기본 점수가 실제 악용 위험을 충분히 설명하지 못하며, PoC 존재 여부 등 추가 요인을 고려할 때 위험 감소 효과가 커짐을 보였다. Jacobs 등[7]은 '공개된 익스플로잇'이 아니라 '실제 악용'을 결과변수로 삼아 조치 전략의 커버리지와 효율성을 비교하였고, 이를 발전시킨 EPSS[5]는 공개 후 악용 확률을 추정하는 개방형 데이터 기반 체계로 제안되었다. 이후 EPSS 3세대 모델[6]은 FIRST(Forum of Incident Response and Security Teams) 특별관심그룹과 다수 기관의 악용 신호를 결합하여 예측 성능을 개선하였다. Suciu 등[10]은 기능하는 익스플로잇이 개발될 가능성을 시간에 따라 예측하는 모델을 제시하였다.

국내에서는 김민철 등[17]이 CVE·CWE·CVSS 등 공개 취약점 정보를 활용한 자동화된 위험도 스코어링 체계를 제안하였고, 공격 코드 성숙도와 시계열 특성을 반영해 산업제어시스템 취약점의 심각도를 재평가한 연구[18]도 수행되었다. 그러나 이들 연구는 KEV 목록 자체의 등재 시점을 분석 대상으로 삼지는 않았다.

2.2 Zero-Day and Time-to-Exploitation Studies

Bilge와 Dumitraş[9]는 1,100만 대 호스트의 현장 데이터를 분석하여 공개 이전에 악용된 취약점 18건을 식별하고, 제로데이 공격이 공개 전 수개월에서 수년간 지속될 수 있음을 보였다. 보안업계 보고서에서도 VulnCheck는 2025년 새로 악용이 확인된 KEV 884건 중 28.96%가 CVE 공개 당일 또는 그 이전에 악용되었다고 보고하였다[14]. Barracuda는 2022년 이후 공개된 CVE의 CISA KEV 등재 소요기간 중앙값을 9일로 제시하며, 오래된 취약점이 섞이면 시차가 실제보다 길어 보인다고 지적하였다[15].

2.3 Studies on KEV Catalogs

KEV를 직접 다룬 최근 연구로, 취약점 관리 연계(chaining) 프레임워크 연구[11]는 KEV 922건과 CVE 28,377건을 분석하여 KEV와 EPSS가 서로 다른 악용 취약점을 포착하는 상호보완 관계임을 보였고, KEV가 악용 이후에야 기록되는 사후적 목록이라는 한계를 지적하였다. 고위험 KEV에서 EPSS의 효과를 분석한 연구[12]는 CVSS 9.0 이상 KEV 90건을 대상으로 등재 이전 EPSS의 예측력을 검토하였으며, 베이지안 위험률 모델 연구[13]는 EPSS의 전역 확률을 조직 단위의 일별 악용 위험률로 변환하고, KEV로 보정한 Weibull 위험률 모형을 제시하였다. runZero의 KEVology 보고서[16]는 CISA KEV의 시간 지표를 종합 분석하였으나 VulnCheck KEV는 분석 범위에서 제외하였다고 명시하였다. VulnCheck의 선행 시간 분석[30]은 2024~2025년 두 목록에 공통으로 등재된 CVE 376건을 비교하여 VulnCheck가 평균 28.13일, 중앙값 3일 먼저 등재하였다고 보고하였으나, 분석 기간이 2년으로 한정되어 관측 기간 불일치가 추정치에 미치는 영향은 다루지 않았다. 즉, 두 KEV 목록의 등재 시점을 전체 기간에 걸쳐 동일 CVE 단위로 비교하고 관측 기간 편향의 크기를 정량화한 연구는 아직 부족하며, 본 연구는 이 공백을 다룬다.

III. Data and Methodology

3.1 Data Collection

본 연구는 Table 2의 다섯 가지 원자료(CISA KEV, VulnCheck KEV, NVD·EPSS·PoC 관측 기록, EPSS 스냅샷, GitHub PoC 공개 시점)를 CVE 식별자로 결합하여, 표의 마지막 행인 통합 데이터셋을 구성하였다. CISA KEV는 공식 카탈로그 CSV(2026년 9월 27일 수집, 등재일 2021-11-03~2026-09-25)를 원출처로 사용하였고, VulnCheck KEV는 자체 개발한 수집 도구에서 필터 없이 내보낸 전체 스냅샷(2026년 9월 25일 18:38 UTC 수집)을 사용하였다.

CVE별 NVD 게시일, CVSS, EPSS, PoC 개수는 자체 개발한 분석 도구의 관측 기록에서 가져왔다. 또한 관측 시점이 서로 다른 EPSS 값을 보완하기 위해 FIRST EPSS API[27]로 2026년 9월 26일 하루 기준의 EPSS를 1,726건

www.kci.go.kr

전체에 대해 다시 수집하였고, GitHub 저장소의 최초 PoC 공개일과 KEV 등재일을 비교하여 등재 이후 처음 PoC가 공개된 262건을 식별하였다.

상세 관측 기록에서 동일 CVE를 여러 번 조회한 경우에는 조회에 성공한 마지막 기록을 사용하여 1,726건을 확보하였으며, NVD 게시일은 최초 조회에 실패한 1건(CVE-2025-48927)을 재조회로 보완하여 1,726건 모두 확보하였다. VulnCheck가 제공하는 CISA 등재일은 공식 카탈로그와 1,725건 모두 일치하였고, 최근 등재된 CVE-2026-87902 1건만 값이 비어 있어 공식 카탈로그 값(2026-09-25)을 적용하였다. 아울러 비교 범위를 공통 관측 기간(2021-11-03 이후)으로 설정한 수집 도구의 별도 산출 결과(2026-09-27)도 본 연구의 W2 결과와 공통 항목 1,113건 전부에서 선행일수가 일치하여 분석의 재현성을 확인하였다. 분석에 사용한 통합 데이터셋과 통계 산출 코드, 그림 생성 스크립트는 공개 저장소[28]에서 확인할 수 있다. 다만, VulnCheck 데이터는 상용 서비스라서 이용자가 직접 받아야 한다.

Table 2. Data Sources

Source	Records	Main Fields
① CISA KEV (official)	1,726	2021-11-03 to 2026-09-25; dateAdded, dueDate, vendor, CWE, ransomware
② VulnCheck KEV	5,361	2000-01-11 to 2026-09-25; date_added, cisa_date_added
③ NVD / EPSS / PoC	1,893 records (1,726 CVEs)	published date, CVSS v3, EPSS, PoC count
④ EPSS snapshot	1,726	EPSS, percentile (2026-09-26)
⑤ GitHub PoC timing	262	first PoC date after KEV listing
Merged dataset (output of ①-⑤)	1,726	CVE-level integrated record

3.2 Variable Definitions and Observation Windows

분석 변수와 관측 기간은 Table 3과 같이 정의하였다. 모든 시차는 날짜 단위(일)로 계산하였으며, 양수는 뒤의 시점이 앞의 시점보다 늦음을 의미한다.

관측 기간 정합화의 핵심은 W2이다. CISA KEV가 존재하지 않던 시기의 VulnCheck 등재일은 구조적으로 CISA보다 앞설 수밖에 없으므로, 두 목록이 모두 운영되던 기간(2021-11-03 이후)의 VulnCheck 등재분만 비교해야 실제 선행성을 추정할 수 있다. W3는 출범 직후의 대량 소급 등재를 제외하기 위한 보조 기준이다.

두 목록의 종료일은 모두 2026년 9월 25일로 같지만, 시작일은 CISA KEV가 2021년 11월 3일, VulnCheck KEV가 2000년 1월 11일로 다르다. VulnCheck 5,361건 중 1,509건(28.1%)이 CISA KEV 출범 이전 등재분이며, 공통 항목 1,726건 중에서도 613건(35.5%)이 이에 해당한다. 따라서 본 연구는 선행일수, 포함 범위, 편입 확률 등 두 목록을 비교하는 모든 핵심 지표를 공통 관측 기간(W2)으로 정합화하여 산출하고, 전체 기간(W0) 결과는 편향의 크기를 보이기 위한 비교 목적으로만 제시하였다.

Table 3. Variables and Observation Windows

Symbol	Definition
ΔCISA	CISA dateAdded − NVD published (CVE-to-CISA lag)
ΔVC	VulnCheck date_added − NVD published
Lead	CISA dateAdded − VulnCheck date_added
Window	dueDate − dateAdded (remediation window)
PoC status	Public PoC before / after listing, or none
EPSS926	EPSS score on 2026-09-26 (uniform date)
W0	All common CVEs (no window alignment)
W1	VulnCheck date_added ≥ 2021-01-01
W2	VulnCheck date_added ≥ 2021-11-03 (CISA KEV launch)
W3	CISA dateAdded ≥ 2023-01-01 (backfill excluded)

3.3 Statistical Methods

시차 변수는 모두 오른쪽으로 크게 치우친 분포를 보여 평균보다 중앙값과 사분위수를 주요 요약값으로 사용하고, 비모수 검정을 적용하였다. 동일 CVE의 두 등재일 비교에는 부호 검정과 Wilcoxon 부호순위 검정을, 연도별 차이에는 Kruskal-Wallis 검정을, 두 집단 비교에는 Mann-Whitney U 검정을, 연속형 지표와 시차의 관계에는 Spearman 순위상관을 사용하였다. 중앙값의 95% 신뢰구간은 5,000회 부트스트랩으로, 비율의 신뢰구간은 Wilson 점수 구간[20]으로 추정하였다. p값과 함께 효과 크기(Wilcoxon r, 순위이연상관 r_rb, ε^2)를 보고하였고, 위험 지표에 대한 7개 검정에는 Holm 방법[26]으로 다중 비교를 보정하였다. 또한 관측 기간 기준일을 2021년 5월부터 2023년 1월까지 바꾸어 가며 결과가 유지되는지 민감도 분석을 수행하였다.

또한 VulnCheck KEV에 등재된 항목이 이후 CISA KEV에 편입되는 시간을 Kaplan-Meier 추정량[21]으로 분석하였다. 대상은 W2 기간에 VulnCheck에 등재된 3,852건이며, CISA 편입을 사건(event)으로, 수집 시점까지 편입되지 않은 2,739건을 중도절단으로 처리하였다. Kaplan-Meier 방법은 중도절단된 항목도 충분히 오래 관

www.kci.go.kr

찰하면 사건이 발생할 수 있다고 가정한다. 그러나 CISA는 명확한 조치 방법이 있는 취약점만 등재하므로 일부 항목은 영원히 편입되지 않을 수 있다. 이에 본 연구는 추정 곡선을 '관측 기간 내 누적 편입 확률'로 해석하고, 곡선이 정체되는 수준을 편입되지 않는 집단의 규모를 가늠하는 지표로 활용하였다. 유의수준은 0.05로 하였다.

IV. Analysis Results

4.1 Dataset Overview

Fig. 1은 연도별 CISA KEV 신규 등재 건수와 조치 기한 중앙값을 보여준다. 2021년 311건 중 287건은 출범일인 11월 3일 하루에 등재되었고, 2022년에도 555건이 등재되어 초기 2년간 과거 취약점의 소급 등재가 집중되었다. 이후 연간 등재 건수는 2023년 187건, 2024년 186건으로 안정되었다가 2025년 245건, 2026년(9월 25일까지) 242건으로 다시 증가하였다.

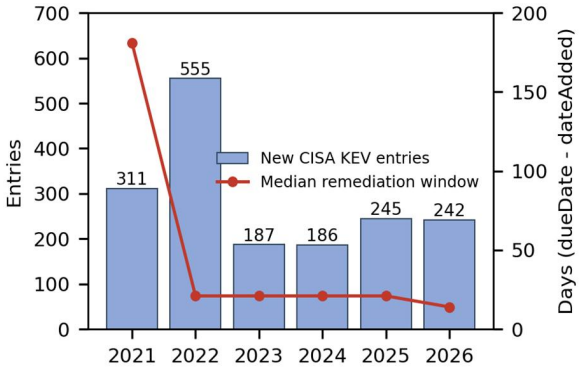


Fig. 1. Yearly CISA KEV Additions and Median Remediation Window

조치 기한 중앙값은 2021년 181일에서 2022~2025년 21일로 짧아졌고, 2026년에는 3월부터 14일, BOD 26-04가 조치 문구에 처음 등장한 2026년 6월 11일 이후에는 3일이 주류가 되었다(6월 이후 등재 119건 중 91건). 벤더별로는 Microsoft(389건), Cisco(99건), Apple(94건), Adobe(82건), Google(75건) 순이었고, CWE 유형은 CWE-20(119건), CWE-78(110건), CWE-787(104건)이 상위를 차지하였다. 공식 카탈로그상 랜섬웨어 악용이 확인된 항목은 361건(20.9%)이었다. CVSS v3 평균은 8.39(중앙값 8.8), 2026년 9월 26일 기준 EPSS 중앙값은 0.490으로, KEV가 고위험 취약점에 집중되어 있음을 확인하였다. 이는 KEV의 평균 CVSS가 전체 취약점보다 높다는 국내 위협 인텔리전스 보고서[19]의 분석과도 일치한다.

4.2 RQ1: Lag from NVD Publication to CISA Listing

Table 4는 NVD 게시일부터 CISA 등재까지의 소요기간(ΔCISA)을 표본 범위별로 요약한 것이다. 전체 표본에서는 평균 861.1일, 중앙값 245.5일로 평균이 중앙값의 3배를 넘었고, 45.4%가 게시 후 1년 이상 지나 등재되었다. 이는 CISA KEV 등재 CVE의 50.8%가 KEV 출범 이전에 게시된 것이며, 17.5%는 게시 후 5년이 지나 등재되었기 때문이다.

Table 4. CVE-to-CISA Lag by Sample (days)

Sample	n	Median [IQR]	Mean	Before NVD (%)
All	1,726	245.5 [8, 1364]	861.1	3.8
Published ≥ launch	849	8 [0, 85]	98.2	7.7
Published ≥ 2023	692	6.5 [0, 55.25]	71.5	4.3
Listed ≥ 2023	860	19 [1, 260.75]	468.8	3.3

반면 KEV 출범 이후 NVD에 게시된 CVE 849건만 보면 중앙값은 8일, 평균은 98.2일로 크게 줄어들고, 49.5%가 게시 후 7일 이내에 등재되었다. 2023년 이후 게시분에서도 중앙값 6.5일, 7일 이내 등재 52.2%로 유사하였다. 이 결과는 Barracuda의 보안업계 보고서[15]가 제시한 중앙값 9일과 일관된다. 즉, "NVD 게시 후 CISA 등재까지 수백 일이 걸린다"는 해석은 오래된 취약점의 소급 등재가 만든 효과이며, 새로 게시된 취약점은 대체로 1~2주 안에 등재된다.

4.3 RQ2: Window-Aligned Coverage of the Two Catalogs

CISA KEV 1,726건은 전부 VulnCheck KEV에 포함되었다. 그러나 두 목록의 포함 범위를 비교할 때에도 관측 기간을 맞추어야 한다. 전체 기간으로 보면 CISA KEV는 VulnCheck KEV 5,361건의 32.2%에 해당하지만, 이 분모에는 CISA KEV가 존재하지 않던 시기의 등재분 1,509건이 포함되어 있다. 공통 관측 기간인 출범일 이후 VulnCheck에 등재된 3,852건만 보면 CISA KEV에도 등재된 항목은 1,113건(28.9%)이고, 나머지 2,739건(71.1%)은 2026년 9월 25일 현재 VulnCheck에만 존재하였다. 즉 기간을 맞추면 공공 목록의 포함 비율은 오히려 낮아진다.

공통 기간의 VulnCheck 단독 항목을 CVE 연도별로 보면

www.kci.go.kr

CVE-2024가 512건, CVE-2023과 CVE-2025가 각각 393건으로 최근 취약점이 많았고, 2021년 이전 CVE는 20.4%였다. 등재 연도 기준으로도 2023~2026년 VulnCheck 단독 신규 등재는 연 460~725건으로, 같은 기간 두 목록의 공통 등재(연 178~212건)의 약 2.5~4배였다. 따라서 두 목록은 대등한 대안이 아니라, CISA KEV가 VulnCheck KEV의 부분집합인 포함 관계이며, 이는 두 목록의 수집 범위와 등재 목적이 다른 데서 비롯된 것으로 해석해야 한다.

4.4 RQ3: Window-Aligned Lead of VulnCheck KEV

Table 5는 관측 기간별 VulnCheck 선행일수를 요약한 것이다. 모든 범위에서 CISA가 먼저 등재한 사례는 0건이었으며, 등재일이 다른 1,282쌍 전부에서 VulnCheck가 먼저였다(부호 검정 $p<0.001$). Wilcoxon 부호순위 검정에서도 W2($n=669$, $z=22.42$, $r=0.87$)와 W3($n=614$, $z=21.48$, $r=0.87$) 모두 큰 효과 크기로 유의하였다($p<0.001$).

Table 5. VulnCheck Lead over CISA by Window (days)

Window	n	Median [95% CI]	Mean	VC first (%)
W0	1,726	15 [11, 23]	526.6	74.3
W1	1,285	3 [2, 4]	65.8	65.4
W2	1,113	2 [1, 2]	41.2	60.1
W3	860	4 [3, 4.5]	248.6	71.4

관측 기간을 정합화한 W2에서 선행일수 중앙값은 2일(95% CI 1~2일), 평균은 41.2일이었다. 같은 날 등재가 39.9%, 1~7일 선행이 30.8%로 전체의 70.7%가 1주일 이내에 집중되었고, 30일을 넘는 선행은 17.6%, 1년을 넘는 선행은 3.1%에 불과하였다. 이는 2024~2025년 공통 항목 376건을 분석한 보안업계 보고서의 중앙값 3일[30]과도 부합한다. 이처럼 대부분의 공통 항목에서 나타나는 수일의 차이는, CISA가 악용 증거를 검증하고 조치 방법을 확인하는 데 필요한 시간으로 해석할 수 있다. CISA 등재 연도별 선행일수는 유의하게 달랐으며(Kruskal-Wallis $H=214.8$, $p<0.001$, $\varepsilon^2=0.12$), 중앙값은 2021년 205일, 2022년 450일에서 2023년 4일, 2024년 5일, 2025년 4일, 2026년 2일로 감소하였다. 벤더별로는 Microsoft($n=189$)와 Cisco($n=84$)의 중앙값이 0일로 두 목록이 거의 동시에 등재하는 반면, Google($n=41$)은 6일로 상대적으로 선행 폭이 컸다.

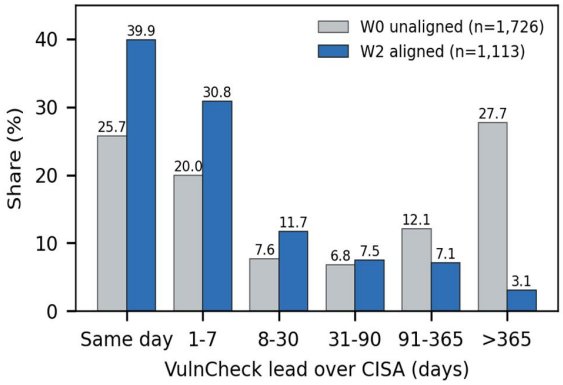


Fig. 2. Distribution of VulnCheck Lead: Unaligned (W0) vs. Aligned (W2)

4.5 RQ4: Magnitude of Observation Window Bias

Fig. 2는 정합화 여부에 따른 선행일수 분포의 차이를 보여준다. 전체 기간(W0)에서는 1년 초과 선행이 27.7%로 가장 큰 구간이었으나, W2에서는 3.1%로 줄었다. 평균은 526.6일에서 41.2일로 약 12.8배, 중앙값은 15일에서 2일로 7.5배 차이가 났다. 이 차이의 원천은 공통 항목 1,726건 중 613건(35.5%)의 VulnCheck 등재일이 CISA KEV 출범 이전에 위치한다는 점이다. 특히 출범일에 소급 등재된 287건은 선행일수 중앙값이 209일로, 이들이 "선행"으로 집계된 것은 CISA가 늦었기 때문이 아니라 목록 자체가 없었기 때문이다.

소급 등재만 제외하는 W3 기준도 평균 248.6일로 여전히 과대 추정되었는데, 이는 2023년 이후 CISA에 새로 추가된 오래된 CVE가 출범 이전의 VulnCheck 등재일을 가지고 있기 때문이다. 따라서 KEV 목록 간 비교에서는 CISA 등재일이 아니라 VulnCheck 등재일을 기준으로 관측 기간을 맞추어야 한다.

기준일 선택이 결론에 영향을 주는지 확인하기 위해 VulnCheck 등재일 기준일을 2021년 5월부터 2023년 1월까지 바꾸어 민감도 분석을 수행하였다(Table 6). 선행일수 중앙값은 모든 기준에서 2~3일, 평균은 39.1~51.1일, 1년 초과 선행 비율은 2.7~3.2%로 거의 변하지 않았고, 30일 내 CISA 편입 확률도 19.7~23.9% 범위에 머물렀다. NVD 게시일 기준일을 같은 방식으로 바꾼 경우에도 Δ CISA 중앙값은 6~15일로 수백 일 규모의 전체 표본 추정치와는 뚜렷이 구분되었다. 따라서 본 연구의 결론은 특정 기준일 선택에 의존하지 않는다.

www.kci.go.kr

Table 6. Sensitivity to the VulnCheck Cutoff Date

Cutoff	n	Median [95% CI]	Mean	CISA in 30 d (%)
2021-05-03	1,210	2 [2, 3]	51.1	22.8
2021-08-03	1,167	2 [2, 3]	43.8	23.2
2021-11-03	1,113	2 [1, 2]	41.2	23.9
2022-02-03	1,011	2 [1, 2]	39.1	22.9
2022-05-03	879	2 [2, 3]	41.8	20.6
2023-01-01	786	3 [2, 3.5]	39.7	19.7

4.6 RQ5: Listing before NVD Publication and Risk Indicators

Fig. 3은 KEV 출범 이후 NVD에 게시된 CVE 849건에 대해 NVD 게시일 대비 두 목록의 등재 시점 분포를 비교한 것이다. CISA 기준 NVD 게시 이전 등재는 7.7%(Wilson 95% CI 6.1~9.6%), 게시 당일 이하 등재는 26.6%였던 반면, VulnCheck 기준 게시 이전 등재는 26.0%, 당일 이하 등재는 54.1%였다. VulnCheck 기준 비율은 VulnCheck 자체 보고서의 28.96%[14]와 유사한 수준이다. 다만 NVD 게시는 벤더 보안 공지보다 며칠 늦는 경우가 많으므로, NVD 게시 이전 등재가 곧 취약점 공개 이전의 악용, 즉 제로데이를 의미하지는 않는다. 본 연구의 음수 시차는 '공식 취약점 데이터베이스에 반영되기 전에 악용 목록에 먼저 올랐다'는 의미로 한정하여 해석해야 한다.

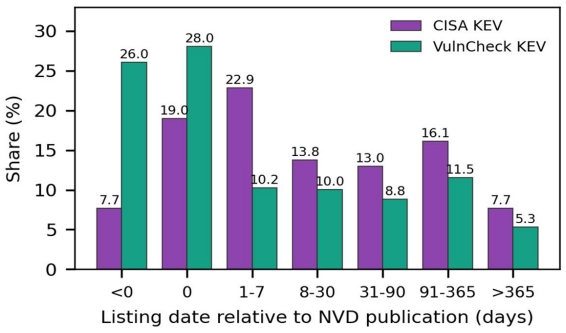


Fig. 3. Listing Timing Relative to NVD Publication (CVEs Published after Launch)

CISA 기준 음수 시차 65건 중 19건은 -1일로 시간대(UTC) 차이에 따른 산출물일 가능성이 있으나, 46건은 -2일 이하로 NVD 게시 전 등재로 볼 수 있다. 음수 사례는 Apple(16건), Google(11건), Microsoft(8건), Android(5건)에 집중되었는데, 이들은 보안 공지에서 악용 사실을 함께 밝히는 경우가 많은 브라우저·모바일 운영체제 벤더이다. Table 7과 같이 게시 당일 이하 등재 비율은 CISA 기준 2022년 36.8%에서 2026년 21.3%로 낮아졌다. 이는 CISA의 대응이 느려졌다기보다, 공개와 동시에 악용되는 취약점보다 공개 이후 악용이 확인되는 취약점의 비중이 커졌음을 시사한다. 다만 2026년은 9월까지의 부분 연도라는 점에 유의해야 한다.

Table 7. Share Listed on or before NVD Publication (%)

Listed year	n	CISA ≤ 0 day	VulnCheck ≤ 0 day
2022	106	36.8	55.7
2023	148	29.7	57.4
2024	155	25.8	58.1
2025	209	23.4	56.5
2026	221	21.3	44.3

Table 8은 위험 지표와 등재 시차의 관계를 효과 크기와 Holm 보정 p값으로 정리한 것이다. KEV 출범 이후 NVD에 게시된 CVE에서 ΔCISA는 CVSS, PoC 개수, 랜섬웨어 악용 여부와 관련이 없었다. CVSS 심각도 등급 간 차이는 보정 전 p=0.047이었으나 보정 후 유의하지 않았고 (p=0.189, ε^2=0.006), EPSS만 약한 양의 상관을 보였다(ρ=0.19). 그러나 EPSS는 등재 이후 시점의 관측값이므로 인과적으로 해석할 수 없다. 전체 KEV에서 랜섬웨어 악용 CVE의 EPSS 중앙값은 0.857로 비악용 CVE(0.410)보다 높았으며 효과 크기도 중간 수준이었다(r_rb=0.35). CVSS와 EPSS의 상관은 Pearson r=0.354, Spearman ρ=0.384로 약한 수준이었다.

Table 8. Risk Indicator Tests (Holm-Adjusted)

Test	Effect size	p	Holm p
CVSS vs ΔCISA	ρ = 0.052	0.131	0.393
EPSS vs ΔCISA	ρ = 0.193	<0.001	<0.001
PoC count vs ΔCISA	ρ = 0.027	0.431	0.861
Ransomware: ΔCISA	r_rb = 0.007	0.891	0.891
Severity: ΔCISA	ε^2 = 0.006	0.047	0.189
Ransomware: EPSS	r_rb = 0.350	<0.001	<0.001
Ransomware: CVSS	r_rb = 0.112	<0.001	0.004

4.7 Survival Analysis of CISA Adoption

Fig. 4와 Table 9는 W2 기간 VulnCheck 등재 3,852건이 이후 CISA KEV에 편입될 누적 확률을 Kaplan-Meier 방법으로 추정한 결과이다. 편입 확률은 등재 당일 11.5%, 7일 20.5%, 30일 23.9%로 초기에 빠르게 증가한 뒤 90일 26.2%, 1년 28.7%, 2년 29.7%로 거의 정체되었다.

www.kci.go.kr

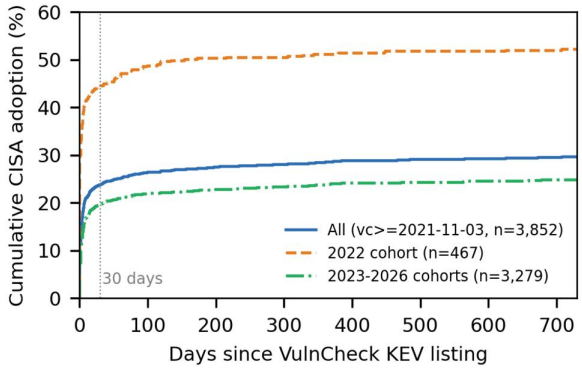


Fig. 4. Kaplan–Meier Estimate of Cumulative CISA Adoption

Table 9. Cumulative CISA Adoption Probability (%)

Days	All (3,852)	2022 (467)	2023–26 (3,279)
0	11.5	30.0	7.5
7	20.5	40.5	16.4
30	23.9	44.5	19.7
90	26.2	48.2	21.8
365	28.7	51.2	24.0
730	29.7	52.2	24.9

30일 이후 2년까지 추가로 편입되는 비율은 5.8%p에 불과하였다. 이는 CISA가 VulnCheck 등재 후 한 달 안에 채택하지 않은 항목은 이후에도 채택할 가능성이 낮다는 것을 의미한다. 코호트별로는 2022년 등재분의 2년 편입 확률이 52.2%였던 반면, 2023~2026년 등재분은 24.9%로 낮아져 VulnCheck의 수집 범위가 넓어질수록 CISA와의 격차가 커지고 있음을 보여준다. 곡선이 약 30% 수준에서 정체된다는 것은, 3.3절에서 설명한 바와 같이 VulnCheck 등재 항목의 약 70%가 CISA의 등재 기준상 편입 대상이 되지 않는 집단일 가능성을 시사하며, 이는 4.3절의 공통 기간 단독 항목 비율(71.1%)과도 부합한다.

4.8 RQ6: Predictive Signals at the Time of Listing

Table 10은 GitHub 최초 PoC 공개일과 KEV 등재일을 비교한 결과이다. 등재 전에 공개 PoC가 있던 항목은 612건(35.5%)에 불과하였고, 852건(49.4%)은 수집 시점까지 PoC가 없었으며, 262건(15.2%)은 등재 이후에 처음 PoC가 공개되었다. 즉 KEV의 64.5%는 등재 시점에 공개 PoC가 없었다. PoC가 있는 항목 중 등재 후 공개된 비율은 전체 30.0%에서 2023년 이후 등재분 38.2%로 높아졌다.

Table 10. Public PoC Status Relative to KEV Listing

PoC status	All (1,726)	Listed ≥ 2023 (860)
Before listing	612 (35.5%)	311 (36.2%)
After listing	262 (15.2%)	192 (22.3%)
└ within 7 days	107 (6.2%)	99 (11.5%)
None	852 (49.4%)	357 (41.5%)

등재 이후 PoC가 공개되기까지의 기간은 중앙값 22일이었고 40.8%가 7일 이내였으며, 2025년 이후 등재분(107건)은 중앙값 2일이었다. 저장소 이름에 해당 CVE 식별자가 포함된 218건으로 한정해도 중앙값 14일, 7일 이내 45.4%로 결과가 유사하였다. 이는 KEV 등재와 공개가 공격 코드의 공개를 앞당기는 '공개 효과'가 존재할 가능성을 시사한다. 다만 본 자료로 인과관계를 확정할 수는 없다.

2026년 9월 26일 기준 EPSS를 보면 KEV의 26.2%가 0.1 미만이었고, 0.5 이상은 49.5%에 그쳤다. 최근 90일 이내 등재된 97건은 EPSS 중앙값이 0.070으로 59.8%가 0.1 미만이었으며, 등재 후 경과일수와 EPSS는 양의 상관을 보였다(ρ=0.198, p<0.001). EPSS 중앙값은 등재 전 PoC가 있던 항목 0.897, 등재 후 PoC 항목 0.283, PoC가 없는 항목 0.225로 유의하게 달랐다(Kruskal-Wallis p<0.001, ε^2=0.18). Fig. 5와 같이 '등재 전 PoC 또는 EPSS 0.1 이상'이라는 신호를 결합해도 KEV의 78.0%만 포착되어, 나머지 22.0%는 두 예측 신호 어디에도 나타나지 않았다. 따라서 예측 신호는 실제 악용 증거에 기반한 등재를 대체할 수 없다.

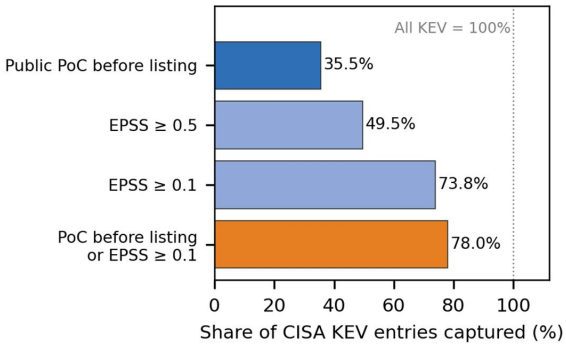


Fig. 5. Share of KEV Entries Captured by PoC and EPSS Signals

4.9 Synthesis of Findings

RQ1~RQ6의 결과를 종합하면 다음 네 가지 통합적 시사점을 얻을 수 있다. 첫째, 등재 시차의 크기는 측정 방법에 크게 좌우된다. NVD 게시 후 수백 일이 걸린다는 결과(RQ1)와 VulnCheck가 수백 일 앞선다는 결과(RQ4)는 모두 KEV 출범 이전 자료가 섞여 생긴 값이며, 관측 기간을

www.kci.go.kr

맞추면 신규 CVE의 CISA 등재는 중앙값 8일, 두 목록의 차이는 중앙값 2일로 줄어든다. 즉 공공 KEV가 크게 느리다는 인식은 상당 부분 측정의 착시이다. 둘째, 두 목록의 실질적 차이는 속도가 아니라 범위에 있다. 공통 항목의 70.7%는 1주일 이내 차이로 등재되지만(RQ3), 공통 기간 VulnCheck 등재분의 71.1%는 CISA에 없고(RQ2), CISA 편입 확률은 30일 이후 거의 늘지 않는다(4.7절). 따라서 민간 목록 항목에 대한 판단은 30일 이내에 이루어져야 하며, 그 이후에는 공공 목록 편입을 기다릴 근거가 약하다.

셋째, 악용은 공식 정보와 예측 신호보다 먼저 나타난다. 신규 CVE의 26.0%는 NVD 게시 전에 VulnCheck에 등재되었고(RQ5), KEV의 64.5%는 등재 시점에 공개 PoC가 없었으며 22.0%는 PoC와 EPSS 어디에도 나타나지 않았다(RQ6). 이는 등재 판단을 공식 데이터베이스나 예측 점수에만 맡길 수 없음을 뜻한다. 넷째, 등재 자체가 새로운 위험 시점이 된다. 등재 이후 처음 공개된 PoC는 2025년 이후 등재분에서 중앙값 2일 만에 나타났으므로(RQ6), 등재와 동시에 짧은 조치 기한과 단계적 정보 공개가 필요하다. 이 네 가지 시사점은 제5장의 상호보완적 운영 방안(Table 12)과 국내형 KEV 설계 기준(Table 13)의 직접적인 근거가 된다.

V. Discussion

5.1 Interpretation of Findings

분석 결과는 두 목록이 경쟁 관계가 아니라 역할이 다른 보완 관계임을 보여준다. 두 목록에 모두 오르는 취약점의 대부분은 같은 날이거나 1주일 이내의 차이로 등재되는데, 이 짧은 차이는 CISA가 악용 증거를 검증하고 조치 방법을 확인한 뒤 등재하는 절차에서 비롯된 것으로 볼 수 있다. 반면 VulnCheck 단독 항목의 대부분은 CISA에 편입되지 않는데, 이는 조치 방법이 명확하지 않거나 연방 기관 대상 조치 의무의 범위 밖에 있는 악용 취약점까지 VulnCheck가 넓게 수집하기 때문으로 볼 수 있다. 따라서 VulnCheck KEV는 '발생 즉시 알리는 경보'의 역할을, CISA KEV는 '검증된 조치 기준'의 역할을 하며, 두 목록의 가치는 속도의 우열이 아니라 대응 단계별 쓰임새로 평가해야 한다.

본 연구의 결과를 기존 연구와 비교하면 Table 11과 같다. 신규 CVE의 CISA 등재 소요기간 중앙값 8일은 Barracuda의 9일[15]과, 관측 기간을 정합화한 VulnCheck 선행일수 중앙값 2일은 2024~2025년 표본의 3일[30]과, NVD 게시 이전 VulnCheck 등재 비율 26.0%는 VulnCheck 보고서의 28.96%[14]와 유사하여, 본 연구의 측정이 기존 결과와 일관됨을 확인하였다.

Table 11. Comparison with Previous Studies

Study	Previous finding	This study
Barracuda [15]	CVEs published since 2022: median 9 d to CISA KEV	Post-launch CVEs: median 8 d (n=849)
VulnCheck [30]	2024-2025, 376 common CVEs: VulnCheck lead median 3 d	2021–2026, window-aligned 1,113 CVEs: median 2 d; unaligned mean overstated 12.8 times
VulnCheck [14]	28.96% of 2025 KEV exploited on or before CVE disclosure	26.0% listed before NVD (VulnCheck) vs 7.7% (CISA)
runZero [16]	Time metrics of CISA KEV only	Paired comparison of two catalogs; CISA adoption 23.9% at 30 d (KM)
Shimizu & Hashimoto [11]	KEV and EPSS are complementary; KEV is retrospective	64.5% had no PoC at listing; 22.0% captured by neither signal
Parla [12] Disclosure	EPSS before listing for 90 KEV with CVSS ≥ 9.0	All 1,726 KEV: 26.2% with EPSS < 0.1

기존 연구와 비교한 본 연구의 차별성은 네 가지이다. 첫째, 기존 보고서는 특정 연도의 표본[30]이나 CISA KEV 단일 목록[15][16]을 다루었으나, 본 연구는 두 목록의 공통 관측 기간 전체를 CVE 단위로 짝지어 비교하였다. 둘째, Barracuda[15]가 오래된 취약점이 NVD-CISA 시차를 부풀린다고 지적한 바 있으나, 두 KEV 목록 간 비교에서 관측 기간 불일치가 선행 효과를 평균 12.8배 부풀린다는 편향의 크기를 정량화하고 민감도 분석으로 검증한 연구는 확인되지 않는다. 셋째, 중도절단을 고려한 생존분석으로 편입 확률이 30일 이후 정체된다는 시간 구조를 밝혔는데, 이는 비율이나 중앙값만 보고한 기존 연구에서는 확인할 수 없는 결과이다. 넷째, 기존 연구가 조직 단위의 우선순위 결정에 머문 것과 달리[11][12], 본 연구는 실증 결과를 국내 CVD/VDP 시범사업과 연계한 제도 설계 기준으로 연결하였다.

5.2 Practical Implications

CISA KEV만 모니터링하는 조직은 공통 항목에 대해서는 대체로 수일 이내의 지연만 겪지만, 공통 관측 기간 동안 VulnCheck에 등재된 항목의 71.1%(2,739건)를 인지하지 못한다. 특히 신규 CVE의 절반 이상이 NVD 게시 당일 이하에 VulnCheck에 등재된다는 점은, 공개 직후의 초기 대응 창을 확보하려면 복수의 KEV 목록을 병행해야

www.kci.go.kr

함을 시사한다. 다만 VulnCheck 단독 항목은 등재 기준이 다를 수 있으므로, EPSS와 자산 노출 정보를 결합한 2차 선별이 필요하다[11]. 이러한 결합 방식은 5.3절에서 구체화한다.

5.3 Complementary Operation of the Two KEV Catalogs

두 목록의 역할 차이를 고려하면, 실무 조직은 Table 12와 같이 두 목록을 네 단계로 결합하여 운영할 수 있다. 1단계(조기 경보)에서는 VulnCheck KEV 등재를 경보로 받아 해당 자산의 노출 여부를 즉시 확인하고, 필요하면 접근 차단 등 임시 완화 조치를 적용한다. 신규 CVE의 54.1%가 NVD 게시 당일 이전에 VulnCheck에 등재되었다는 결과는 이 단계가 공개 직후의 대응 시간을 확보해 준다는 것을 보여준다. 2단계(선별)에서는 VulnCheck 단독 항목을 자산 노출, 등재 전 PoC, EPSS, 랜섬웨어 악용 정보로 선별하여 조치 순서를 정한다. 3단계(조치 의무)에서는 CISA KEV 등재를 검증된 조치 기준으로 삼아 정해진 기한 안에 패치를 완료한다. 공통 항목의 70.7%가 1주일 이내의 차이로 두 목록에 오르므로, 1단계에서 미리 준비한 조직은 CISA 등재 시점에 곧바로 조치에 들어갈 수 있다. 4단계(30일 검토)에서는 30일이 지나도 CISA에 편입되지 않은 항목을 더 이상 CISA 편입을 기다리지 않고 조직 자체의 위험 판단으로 조치 여부를 결정한다. 30일 이후 2년까지 추가 편입이 5.8%p에 그친다는 결과가 이 검토 시점의 근거이다.

이 방식에서 VulnCheck KEV는 '무엇을 먼저 살펴볼 것인가'를, CISA KEV는 '무엇을 반드시 기한 안에 조치할 것인가'를 알려준다. 국내형 KEV도 이러한 경보와 조치 기준의 두 역할을 하나의 체계 안에 담도록 설계할 수 있으며, 5.5절의 설계 기준은 이 운영 방안을 국내 제도로 옮긴 것이다.

Table 12. Complementary Operation of VulnCheck KEV and CISA KEV

Stage	Source and action	Evidence in this study
S1 Early warning	VulnCheck KEV listing: check asset exposure within 24 h; apply temporary mitigation	54.1% of new CVEs listed by VulnCheck on or before NVD date
S2 Triage	Prioritize VulnCheck-only entries by exposure, prior PoC, EPSS ≥ 0.1, ransomware use	PoC or EPSS signals capture 78.0% of KEV
S3 Mandatory action	CISA KEV listing: remediate by the due date (3-21 days)	VulnCheck lead median 2 d; 70.7% within 7 d
S4 30-day review	Not adopted by CISA within 30 days: decide by organizational risk	Adoption 23.9% at 30 d; only +5.8%p by 2 y

5.4 Methodological and Policy Implications

방법론적으로 KEV 목록을 비교하는 연구와 보안업계의 분석 보고서는 관측 기간을 명시하고 정합화 해야 한다. 정합화 하지 않으면 선행 효과가 평균 기준 10배 이상 과대추정될 수 있으며, 이는 공공 목록의 대응 속도를 실제보다 나쁘게 평가하게 만든다. 정책적으로는 국내 CVD/VDP 로드맵[22]이 신고·조치·공개 단계를 다루고 있는 만큼, 그 다음 단계인 '악용 증거 기반 우선순위' 체계를 함께 설계할 필요가 있다. 구체적인 제언은 제6장에서 정리한다.

5.5 Design Criteria for a Korean KEV Linked to the CVD/VDP Pilot

이상의 결과와 5.3절의 운영 방안을 바탕으로 국내형 KEV(K-KEV)의 설계 기준을 Table 13과 같이 제안한다. 각 기준은 본 연구의 실증 결과에 근거하며, 2026년 6월 시작된 CVD/VDP 시범사업에서 검증할 수 있도록 측정 가능한 형태로 제시하였다.

Table 13. Design Criteria for a Korean KEV (K-KEV)

Criterion	Design standard	Evidence in this study
C1 Listing basis	Confirmed exploitation evidence required; EPSS and PoC used only as auxiliary signals	64.5% had no PoC at listing; 26.2% had EPSS < 0.1
C2 Listing speed	Median ≤ 7 days from exploitation confirmation to listing	New CVEs: CISA median 8 d; VulnCheck lead median 2 d
C3 Source diversity	Combine CVD reports, KISA incident data, and public/private foreign KEVs	CISA KEV covers 28.9% of VulnCheck KEV (common period)
C4 Review window	Decide on foreign-KEV candidates within 30 days and record reasons	CISA adoption 23.9% at 30 d vs 29.7% at 2 y
C5 Deadline	Dual track: 90 days for CVD reports; 3-14 days for K-KEV entries	CISA 3 d after BOD 26-04; 40.8% of late PoCs within 7 d
C6 Disclosure	Staged disclosure; technical details withheld until patch or deadline	Post-listing PoC median 2 d (listed 2025-26)
C7 Metrics	Window-aligned lag indicators with standard timestamps	Unaligned mean overstated 12.8 times

7개 기준은 K-KEV가 하나의 악용 취약점을 처리하는 운영 주기, 즉 등재 판단(C1), 등재(C2), 출처 결합(C3), 해외 KEV 후보 검토(C4), 조치(C5), 공개(C6), 성과 측정(C7)의 순서에 따라 도출하였다. 설계 항목은 CISA BOD 22-01·26-04의 등재 요건과 조치 기한[2][3], 국내

www.kci.go.kr

CVD/VDP 로드맵의 신고·조치·공개 단계[22]를 결합하여 정하였고, 각 항목의 기준값은 본 연구의 실증 결과로 정하였다. C1은 RQ5·RQ6, C2는 RQ1·RQ3, C3는 RQ2, C4는 4.7절의 생존분석, C5와 C6은 RQ6의 등재 후 PoC 공개 결과, C7은 RQ4에 근거한다. 따라서 모든 기준은 하나 이상의 실증 결과와 연결되며, 실증 근거가 없는 항목은 포함하지 않았다.

C1은 가장 중요한 기준이다. 공개 PoC나 EPSS를 등재 요건으로 삼으면 실제 악용된 취약점의 상당 부분을 놓치게 되므로, 등재는 악용 증거로 판단하고 예측 신호는 등재 후보를 빠르게 선별하는 보조 수단으로 활용해야 한다. C2와 C4는 등재 속도와 검토 기한을 정한 것으로, 해외 목록의 편입이 대부분 30일 안에 이루어진다는 결과를 반영하였다. C5와 C6은 로드맵의 90일 조치·공개 원칙[22]을 유지하면서, 악용이 확인된 취약점에는 짧은 조치 기한을 적용하고 공개 직후 공격 코드가 확산될 위험을 고려해 기술 정보를 단계적으로 공개하자는 것이다.

이 기준을 시범사업에서 검증하려면 Table 14의 항목을 신고 건마다 표준화된 형식으로 기록해야 한다. 특히 C4를 검증하기 위해 해외 KEV 후보별로 검토 일자, 편입 여부와 사유를 기록한다. 현행 신고포상제에서는 신고 이후 조치·공개 단계의 날짜가 체계적으로 남지 않아 2,525건의 신고 중 공개 3건이라는 결과 외에는 평가 근거가 부족하였다[22]. 시범사업 단계에서 이 항목들을 확보하면, 본 연구와 같은 방식으로 해외 KEV와 정합화된 비교가 가능해진다.

Table 14. Data Items to Collect in the CVD/VDP Pilot

Data item	Use for K-KEV
Report received / vendor notified	Baseline for CVD lead time
Patch released / disclosed / CVE ID	Disclosure-to-listing lag
Exploitation evidence (Y/N, source, date)	Listing trigger (C1)
K-KEV listing date / deadline	Speed and deadline indicators (C2, C5)
First public PoC date	Disclosure effect monitoring (C6)
EPSS at report and at listing	Auxiliary triage (C1)
CISA / VulnCheck listing dates	Window-aligned benchmarking (C3, C7)
Foreign-KEV review (date, decision, reason)	Review-window compliance (C4)
Remediation completion date	On-time remediation rate

시범사업의 핵심 성과지표로는 (1) 악용 확인부터 K-KEV 등재까지의 중앙값, (2) 조치 기한 내 완료율, (3) 관측 기간을 정합화한 해외 KEV 대비 선후행일수, (4) 신고에서 조치·공개로 이어진 전환율을 제안한다. 시범사업 참여 기관이 15개로 제한적인 만큼, 초기에는 해외 KEV와의 비교 지표를 함께 산출하여 국내 운영 수준을 상대적으로 평가하는 것이 현실적이다.

5.6 Limitations

본 연구에는 다음과 같은 한계가 있다. 첫째, 같은 날 등재가 두 목록의 독립적 발견을 의미하지 않으며, VulnCheck가 CISA 발표를 반영했을 가능성이 있다. 둘째, VulnCheck의 등재일은 최초 악용 증거 시점을 소급 기록했을 수 있다. 셋째, EPSS는 2026년 8월 28일~9월 26일의 관측값으로 등재 이후 시점의 값이므로 사후 편향이 존재한다[12]. 넷째, 랜섬웨어 악용 표기는 사후에 추가되는 경향이 있어 최근 연도의 비율(2025년 12.7%, 2026년 11.2%)이 과소 집계되었을 수 있다. 다섯째, 날짜 단위 비교로 인한 시간대 오차가 존재한다. 여섯째, NVD 게시일을 기준 시점으로 사용하여 벤더 보안 공지일을 반영하지 못하였으므로 음수 시차를 제로데이 악용으로 해석하는 데에는 한계가 있다. 일곱째, Kaplan-Meier 추정은 편입되지 않는 집단의 존재를 명시적으로 모형화하지 않았으며, 향후 치유 모형(cure model) 등으로 보완할 필요가 있다. 여덟째, PoC는 GitHub 저장소만을 대상으로 저장소 생성일을 기준으로 식별하였으므로 비공개 익스플로잇이나 다른 플랫폼의 공개 코드는 반영하지 못했고, 일부 저장소는 실제 PoC가 아닐 수 있다. 아홉째, EPSS 스냅샷 역시 등재 이후 시점의 값이어서 등재 당시의 예측력을 직접 평가한 것은 아니다.

VI. Conclusions

본 연구는 CISA KEV 공식 카탈로그 1,726건과 VulnCheck KEV 전체 5,361건을 NVD·EPSS·GitHub PoC 자료와 통합하여 NVD 게시와 KEV 등재 간 시차를 실증 분석하였다. 두 목록의 시작일이 다르므로 모든 비교 지표는 공통 관측 기간으로 정합화하였다. 새로 게시된 CVE의 CISA 등재 소요기간 중앙값은 8일이었고, CISA KEV는 VulnCheck KEV의 부분집합이면서도 공통 기간 VulnCheck 등재분의 28.9%만 포함하였다. 관측 기간을

www.kci.go.kr

정합화하면 VulnCheck의 선행일수 중앙값은 2일로, 단순 비교의 수백 일 선행은 CISA KEV 출범 이전 등재일에서 비롯된 착시였으며 이 결과는 민감도 분석에서도 유지되었다. VulnCheck 등재 항목이 CISA에 편입될 확률은 30일 이후 거의 증가하지 않았다. 또한 KEV의 64.5%는 등재 시점에 공개 PoC가 없었고, PoC와 EPSS를 결합해도 22.0%는 어떤 예측 신호에도 나타나지 않았다. 기존 연구와 비교하면(Table 11), 이러한 측정값은 보안업계 보고서의 결과(CISA 등재 중앙값 9일[15], VulnCheck 선행 중앙값 3일[30])와 일관되면서도, 본 연구는 두 목록의 공통 관측 기간 전체를 짝지어 비교하고 관측 기간 편향을 정량화했으며, 생존분석과 예측 신호 분석을 결합해 그 결과를 국내 제도 설계로 연결했다는 점에서 차별성을 갖는다.

두 목록의 시차는 우열이 아니라 등재 목적과 검증 절차의 차이에서 비롯되므로, 본 연구는 먼저 VulnCheck KEV를 조기 경보로, CISA KEV를 검증된 조치 기준으로 삼아 경보-선별-조치-검토의 4단계로 결합하는 상호보완적 운영 방안(Table 12)을 제시하였다. 이어서 국내 CVD/VDP 도입 로드맵[22]과 연계한 국내형 KEV의 7대 설계 기준(Table 13)을 제안하였다. 핵심은 네 가지이다. 첫째, 등재는 실제 악용 증거에 근거하고 PoC와 EPSS는 보조 신호로 활용한다. 둘째, 민간 KEV의 조기 경보 기능과 공공 KEV의 검증된 조치 기능을 단계적으로 결합하고, 여기에 CVD 신고 정보를 더한다. 공통 관측 기간 기준으로 CISA KEV가 VulnCheck KEV 항목의 28.9%만 포함한다는 결과는 단일 출처의 한계를 보여준다. 셋째, 일반 신고 취약점의 90일 조치 원칙과 별도로, 악용이 확인된 취약점에는 3~14일의 단축 기한을 두는 이원적 체계를 운영한다. 넷째, 등재 후 공격 코드가 빠르게 공개되는 경향을 고려해 기술 정보를 단계적으로 공개한다.

이러한 기준은 2026년 6월부터 진행 중인 시범사업에서 검증되어야 한다. 이를 위해 시범사업은 신고 접수일, 기관 통보일, 패치·공개일, 악용 증거와 확인일, 최초 PoC 공개일, 등재 시점 EPSS, 해외 KEV 등재일을 표준화된 형식으로 기록해야 하며(Table 14), 악용 확인에서 등재까지의 시차와 기한 내 조치율 등 성과지표는 관측 기간을 정합화한 방식으로 산출해야 한다. 미국이 VDP 의무화(BOD 20-01)[23] 다음 해에 KEV(BOD 22-01)[2]를 도입하여 '발견'과 '우선 조치'를 연결하였듯이, 국내에서도 CVD 관리 전문기관으로 거론되는 KISA가 신고·공개 정보와 악용 증거를 함께 관리하는 구조가 바람직하다.

향후 연구에서는 시범사업에서 수집된 신고·조치·공개 자료를 본 연구의 분석 틀에 적용하여 제안한 설계 기준의 타당성을 검증하고, 기준값(등재 목표 7일, 검토 기한 30일, 단축 조치 기한 3~14일)을 국내 실정에 맞게 조정할 계획이다. 아울러 스냅샷 반복 수집을 통한 전향적 추적, 등재 이전 시점의 EPSS 이력과 벤더 보안 공지일을 활용한 등재 시점 예측 모델과 치유 모형 구축을 병행하고자 한다.

ACKNOWLEDGEMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT)(IITP-2026-RS-2022-00156334).

REFERENCES

[1] CISA, "Known Exploited Vulnerabilities Catalog," Cybersecurity and Infrastructure Security Agency, 2026. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog (accessed Sep. 27, 2026).*

[2] CISA, "Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities," Cybersecurity and Infrastructure Security Agency, Nov. 3, 2021. *https://www.cisa.gov/binding-operational-directive-22-01*

[3] CISA, "Binding Operational Directive 26-04: Prioritizing Security Updates Based on Risk," Cybersecurity and Infrastructure Security Agency, Jun. 10, 2026. *https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk*

[4] VulnCheck, "VulnCheck KEV: Known Exploited Vulnerabilities," VulnCheck Inc., 2026. *https://www.vulncheck.com/kev (accessed Sep. 25, 2026).*

[5] J. Jacobs, S. Romanosky, B. Edwards, M. Roytman, and I. Adjerid, "Exploit Prediction Scoring System (EPSS)," Digital Threats: Research and Practice, Vol. 2, No. 3, 2021. DOI: 10.1145/3436242

[6] J. Jacobs, S. Romanosky, O. Suciu, B. Edwards, and A. Sarabi, "Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights," Proc. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 194-206, 2023. DOI: 10.1109/EuroSPW59978.2023.00027

[7] J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, "Improving Vulnerability Remediation through Better Exploit Prediction," Journal of Cybersecurity, Vol. 6, No. 1, tyaa015, 2020. DOI:

www.kci.go.kr

10.1093/cybsec/tyaa015

[8] L. Allodi and F. Massacci, "Comparing Vulnerability Severity and Exploits Using Case-Control Studies," ACM Transactions on Information and System Security, Vol. 17, No. 1, 2014. DOI: 10.1145/2630069

[9] L. Bilge and T. Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," Proc. 2012 ACM Conference on Computer and Communications Security (CCS), pp. 833-844, 2012. DOI: 10.1145/2382196.2382284

[10] O. Suciu, C. Nelson, Z. Lyu, T. Bao, and T. Dumitras, "Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits," Proc. 31st USENIX Security Symposium, USENIX Association, pp. 377-394, 2022. *https://www.usenix.org/conference/usenixsecurity22/presentation/suciu*

[11] N. Shimizu and M. Hashimoto, "Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization," IEEE Access, Vol. 14, pp. 31407-31424, 2026. DOI: 10.1109/ACCESS.2026.3665768

[12] R. Parla, "Efficacy of EPSS in High Severity CVEs found in KEV," arXiv:2411.02618, 2024. DOI: 10.48550/arXiv.2411.02618

[13] S. Shaffer and L. Voicu, "Modeling Local Exploit Hazard - A Bayesian Framework for Quantifying Exploit Risk and Operational Efficiency," arXiv:2607.24618, 2026. DOI: 10.48550/arXiv.2607.24618

[14] P. Garrity, "State of Exploitation 2026," VulnCheck, 2026. *https://www.vulncheck.com/blog/state-of-exploitation-2026*

[15] A. Kjoelen, "The KEV Gap: How Fast Do Exploited Bugs Get Flagged?," Barracuda Blog, Jul. 24, 2026. *https://blog.barracuda.com/2026/07/24/KEV-gap-how-fast-do-exploited-bugs-get-flagged*

[16] T. Beardsley, "KEVology: An Analysis of CISA KEV Exploits, Scores, & Timelines," runZero, Feb. 2026. *https://www.runzero.com/resources/kevology/*

[17] Min Cheol Kim, Sejoon Oh, Hyunjae Kang, Jinsoo Kim, and Huy Kang Kim, "Risk Scoring System for Software Vulnerability Using Public Vulnerability Information," Journal of the Korea Institute of Information Security & Cryptology, Vol. 28, No. 6, pp. 1449-1461, 2018. DOI: 10.13089/JKIISC.2018.28.6.1449

[18] S. S. Yoon and I. C. Euom, "A Study on Vulnerability Severity Evaluation Considering Attacker Skill Level Based on Time Series Characteristics," Journal of the Korea Institute of Information Security & Cryptology, Vol. 33, No. 2, pp. 281-293, 2023. DOI: 10.13089/JKIISC.2023.33.2.281

[19] S2W Threat Intelligence Center (TALON), "Recent Trends in Known Exploited Vulnerabilities (KEV)," S2W, Dec. 30, 2025. *https://s2w.inc/en/resource/detail/988*

[20] E. B. Wilson, "Probable Inference, the Law of Succession, and Statistical Inference," Journal of the American Statistical Association, Vol. 22, No. 158, pp. 209-212, 1927. DOI: 10.1080/01621459.1927.10502953

[21] E. L. Kaplan and P. Meier, "Nonparametric Estimation from Incomplete Observations," Journal of the American Statistical Association, Vol. 53, No. 282, pp. 457-481, 1958. DOI: 10.1080/01621459.1958.10501452

[22] National AI Strategy Committee of Korea, "Roadmap for Introducing a Security Vulnerability Reporting, Remediation, and Disclosure System (CVD/VDP)," Agenda 3, 2nd Plenary Meeting, Feb. 25, 2026. *https://www.aikorea.go.kr/web/board/brdDetail.do?menu_cd=000012&num=325*

[23] CISA, "Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy," Cybersecurity and Infrastructure Security Agency, Sep. 2020. *https://www.cisa.gov/binding-operational-directive-20-01*

[24] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS 2 Directive)," Official Journal of the European Union, L 333, pp. 80-152, Dec. 2022. h*ttp://data.europa.eu/eli/dir/2022/2555/oj*

[25] European Parliament and Council of the European Union, "Regulation (EU) 2024/2847 of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act)," Official Journal of the European Union, L series, 2024/2847, Nov. 2024. *http://data.europa.eu/eli/reg/2024/2847/oj*

[26] S. Holm, "A Simple Sequentially Rejective Multiple Test Procedure," Scandinavian Journal of Statistics, Vol. 6, No. 2, pp. 65-70, 1979.

[27] FIRST, "Exploit Prediction Scoring System (EPSS)," Forum of Incident Response and Security Teams, 2026. *https://www.first.org/epss/ (accessed Sep. 26, 2026).*

[28] Seung Han Yoon and Ah Reum Kang, "Listing Time Lags between CISA KEV and VulnCheck KEV and Design Criteria for a Korean KEV," GitHub Repository, 2026. *https://github.com/newlife-wq/KEV* DOI: 10.5281/zenodo.23021391

[29] Boannews, "White Hackers to Search for Vulnerabilities without Fear of Punishment: Pilot Program for Continuous Security Vulnerability Reporting Launched," May 28, 2026 (in Korean). *http://www.boannews.com/media/view.asp?idx=143845*

[30] VulnCheck, "What 28 Days of Faster Vulnerability Intelligence Is Worth," VulnCheck Blog, 2026. *https://www.vulncheck.com/blog/economic-value-lead-time*

www.kci.go.kr

Authors



Seung Han Yoon obtained a bachelor's degree in Information Security through the Korean Academic Credit Bank System in 2022. His major experiences include serving as the head of the integrated security control team at the Gyeongsangnam-do Office of Education (from 2012 to 2016), Director of the Cyber Safety Center at Korea Midland Power and Korea Land & Housing Corporation (from 2016 to 2019), Information Security Team Leader at the Korea Forest Welfare Agency (from 2019 to 2020), and Director of the Cyber Security Talent Center at the Korea Internet & Security Agency (from 2021 to 2022). Currently, he works as the head of the technology infringement analysis team at the Defense Agency for Technology and Quality.



Ah Reum Kang received the M.S. and Ph.D. degrees in information security from Korea University, South Korea, in 2012 and 2016. She is a professor in the Department of Information Security at Pai Chai University in Daejeon, South Korea. Her current research interests include security, artificial intelligence, malware, medical data analysis, and online game security.

www.kci.go.kr