디지털산업정보학회 논문지 제19권 제2호-2023년 6월
http://dx.doi.org/10.17662/ksdim.2023.19.2.039

클라우드 서비스 보안성 향상을 위한 CVE 개선 방안 연구

김 태 경* · 정 성 민**

A Study on CVE Improvement Plans to improve Cloud Service Security

Kim Taekyung · Jung Sungmin

〈Abstract〉

The rise in popularity of cloud services has brought about a heightened concern for security in the field of cloud computing. As a response, governments have implemented CSAP(Cloud Security Assurance Program) to ensure the security of these services. However, despite such measures, the emergence of various security vulnerabilities persists, resulting in incidents related to cloud security breaches. To address this, the utilization of Common Vulnerabilities and Exposures (CVE) has been proposed as a means to facilitate the sharing of vulnerability information across different domains. Nevertheless, the unique characteristics of cloud services present challenges in assigning CVE IDs to the diverse range of vulnerabilities within the cloud environment.

In this study, we analyzed how CVE can be effectively employed to enhance cloud security. The assignment of a CVE ID is contingent upon the fulfillment of three rules in the Counting Decision and five rules in the Inclusion Decision. Notably, the third rule in the Inclusion Decision, INC3, clashes with the nature of cloud services, resulting in obstacles in assigning CVE IDs to various cloud vulnerabilities. To tackle this issue, we suggest the appointment of designated individuals who would be responsible for overseeing specific areas of cloud services, thereby enabling the issuance of CVE IDs. This proposed approach aims to overcome the challenges associated with the unique characteristics of cloud services and ensure the seamless sharing of vulnerability information. Information sharing regarding vulnerabilities is crucial in the field of security, and by incorporating cloud vulnerabilities into the CVE system, this method can contribute to enhancing the security of cloud services.

Key Words : Cloud Service, Vulnerability, CVE, Security Management

Ⅰ. 서론

클라우드 서비스[1]는 더욱 활성화되고 있으며, 이에 따라 다양한 해킹사고가 발생하고 있다. 가트너의 자료에 의하면 우리나라의 2023년 퍼블릭 클라우드 서비스 지출액이 올해 5조 1,600억원에서 23.7% 증가한 6조 4,700억원에 육박할 것이라 추산했다. 또, 가트너는 국내 시장에서 BPaaS(Business Process as a Service),

* 명지전문대학 인터넷보안공학과 교수(제1저자)
** 명지전문대학 인터넷보안공학과 교수(교신저자)

PaaS(Platform as a Service), SaaS(Software as a Service), DaaS(Desktop as a Service), IaaS (Infrastructure as a Service) 등 모든 부문이 다음 해에는 두 자릿수 성장률을 기록할 것으로 전망했다[2].

클라우드 서비스가 활성화됨에 따라 클라우드 서비스 장애도 증가하고 있는데, 클라우드 서비스는 인프라(IaaS)에 장애가 발생할 경우 이를 이용하는 클라우드 서비스(SaaS, PaaS, DaaS 등)도 같이 장애가 발생하는 특징을 가지고 있다. 우리나라에서는 클라우드 서비스 안전성 및 신뢰성 확보를 위하여 클라우드 보안인증제(CSAP, Cloud Security Assurance Program)를 시행하고 있다. 클라우드 보안인증 절차는 크게 3단계로 진행된다. 신청기관이 클라우드 시스템 및 서비스를 구축하고 평가·인증 신청 및 계약을 준비하는 준비단계, 신청 서비스를 대상으로 서면/현장 평가, 취약점 점검, 모의침투 테스트를 수행한 후 그 결과 발견된 부적합사항 및 취약점을 신청기관이 보완조치(보완조치기간 : 1-3개월)하는 평가단계, 인증위원회가 평가 결과를 심의하여 인증서를 교부하는 인증단계 순으로 진행된다[3].

클라우드 보안인증제에서 61개 업체에 대한 CSAP 인증 최초평가 결과 발견된 서면/현장 평가 부적합사항에 의하면[3], 네트워크 보안 분야에 59건, 데이터 보호 및 암호화 분야 55건, 가상화 보안 54건, 접근통제 54건, 준거성 49건, 시스템 개발 및 도입 보안 48건, 공공기관 보안요구사항 45건, 침해사고 관리 40건, 서비스 연속성 관리 32건, 인적보안 16건, 정보보호 정책 및 조직 15건, 자산관리 10건, 물리적 보안 7건, 서비스 공급망 관리 분야에 6건이 부적합한 것으로 조사되었다. 따라서, 클라우드 서비스의 보안성 향상을 위해서는 기존에 알려진 자주 발생하는 취약점에 대한 보완조치를 철저히 이행하고, 새롭게 발생하는 보안 취약점을 주기적으로 조사하여, 조기에 발견하고 이에 대응하는 관리활동을 수행해야 한다. 특히, 새롭게 발생하는 취약점을 보안관리에 적용하기 위해 CVE를 활용하는 다양한 연구들이 수행되고 있다[4-6]. CVE 이외에도 취약점과 관련된 CWE(Common Weakness Enumeration), CVSS(Common Vulnerability Scoring System)가 있는데, CWE는 프로그래밍 언어인 C, C++, Java 및 아키텍처, 설계, 코딩 등에서 발생하는 취약점 목록을 정의하는 것이며[7], CVSS는 하드웨어와 소프트웨어 플랫폼 전체에 걸쳐서 취약점을 등급으로 나누어 점수화하는 방식이다[8].

위험분석 및 평가를 위해서는 CVE가 사용되고 있으며, CVE(Common Vulnerabilities and Exposures)[9]는 일반적으로 사용되는 취약점 식별 체계이다. 이는 컴퓨터 시스템, 소프트웨어, 네트워크 장비 등 다양한 IT 제품 및 서비스에서 발견된 취약점에 고유한 식별자를 부여하는 방법을 제공한다. CVE는 취약점에 대한 표준 식별 체계로서, 모든 관련 이해 관계자들이 동일한 식별자를 사용하여 특정 취약점에 관해 이야기할 수 있도록 지원한다. CVE의 주요 목적은 다음과 같다.

① 취약점 식별: CVE는 취약점을 고유하게 식별하기 위한 체계이다. 각 취약점은 CVE 식별자를 통해 고유하게 식별되며, 이를 통해 해당 취약점에 대한 공유와 토론이 가능해진다.
② 취약점 공개와 협업: CVE는 취약점을 공개적으로 보고하고 다른 보안 전문가 및 조직들과 협업하는 데 사용된다. CVE를 통해 발견된 취약점에 대한 정보를 공유함으로써 전체 보안 커뮤니티가 취약점에 대응할 수 있다.
③ 취약점 관리: CVE는 취약점 관리 및 보완조치에 필요한 정보를 제공한다. 각 CVE 식별자는 취약점의 특정 버전, 영향을 받는 제품 등을 식별하는 데 도움이 된다.
④ CVE는 취약점 관리 및 보안 커뮤니티에서 중요한 역할을 하고 있으며, 취약점 보고서, 보안 패치, 취약점 데이터베이스 등 다양한 관련 자료와 함께 사용된다.

우리나라에서도 한국인터넷진흥원에서 보안 취약점 사전 발굴 및 조치를 위해 사이버 보안 취약점 정보 포털 사이트를 운영하고 있다[10]. 그러나 현행 CVE 시스템에는 모든 클라우드 환경에 걸친 취약점의 전체 목록이 포함되지 않는 단점을 가지고 있다. 즉, CSP가 자체적으로 발행하는 패치는 대체적으로 CVE 시스템 내에 캡처되지 않고 있는 상황이다[11]. 따라서 클라우드 보안 서비스를 효과적으로 구축하기 위해서는 CVE 정보 이외에 클라우드 문제를 추적하고 해결할 방법론을 개발해야 한다는 문제점이 발생하게 된다.

따라서 본 논문에서는 클라우드 보안성 향상을 위한 CVE 개선 연구를 수행하였으며, 2장에서는 CVE ID 부여 절차 및 방법에 대해 소개하고, 3장에서는 클라우드 취약점 제공을 위한 CVE 개선 방안에 관해 설명하다. 마지막으로 4장에서는 본 연구의 결론으로 구성하였다.

II. CVE ID 부여 절차 및 방법

CVE ID는 CVE Numbering Authority (CNA) 규칙을 통해 CVE ID 할당에 대한 요구 사항을 정의한다. 요구 사항은 세 가지의 Counting Decision과 다섯 가지의 Inclusion Decision 규칙으로 나누어진다. Counting Decision은 보고된 취약점의 수를, Inclusion Decision은 CVE ID 할당 여부와 할당을 담당할 주체를 결정하는 데 도움을 준다[12].

2.1 Counting Decision

첫 번째 규칙(CNT1)인 CNT1은 보고된 취약점들을 독립적으로 수정 가능한 버그로 분할해야 한다는 것이다. CVE 프로그램은 취약점을 계산하는 방식이 보고자와 다를 수 있으므로, 처리 규칙은 취약점을 기본 구성 요소로 분해하는 것으로 시작한다. 이렇게 함으로써 각 취약점이 하나의 CVE ID만 받고, 중복된 할당이 없도록 보장한다. 간단히 말해, 취약점을 완화하기 위해 여러 버그를 수정해야 하거나 한 버그를 수정함으로써 다른 버그로 인한 취약점이 없어지는 경우, 이러한 버그들은 독립적으로 수정 가능한 것으로 간주하지 않고 함께 그룹화되어야 한다. 독립적으로 수정 가능한지에 대한 불확실성이 있는 경우에도 버그들은 함께 그룹화되어야 한다. 독립적으로 수정 가능성을 기준으로 취약점을 평가함으로써 CVE 프로그램은 일관성을 유지하고 중복된 할당을 피하며 취약점의 정확한 식별과 추적에 기여한다.

두 번째 규칙(CNT2)은 첫 번째 규칙에서 확인된 사항이 취약점인지를 확인하는 단계이다. 취약점이라고 주장하는 주체를 Product Owner, Reporter, CNA(CVE Numbering Authority)로 나눌 수 있는데, 소프트웨어 공급 업체, 하드웨어 공급 업체, 오픈 소스 프로젝트 및 서비스 제공 업체 등 Product owner가 취약점이라고 확인한 사항은 취약점이라고 인정하며, Product owner는 자신의 제품에 취약점이 있는 것을 명확하게 진술해야 하며, 해당 진술에는 취약점을 인정하는 데에 충분한 정보가 포함되어야 한다.

그러나 소프트웨어 소유자가 취약점을 인정하지 않는 경우, 소프트웨어 소유자가 해당 취약점이 아니라고 주장하는 경우, 소프트웨어 소유자에게 연락할 수 없는 경우, 소프트웨어 소유자가 누구인지 확실하지 않은 경우도 발생할 수 있으므로 이런 경우에는 Reporter 또는 CNA에 의해서 취약점이라고 판단해야 하는데, Reporter는 취약점을 보고한 사람이 해당 취약점에 대한 부정적인 영향을 설명하는 것이며, 이를 보고자의 주장을 기반으로 한 클레임 기반 모델이라고 하고, CNA가 보안 정책 위반을 확인하는 것을 정책 기반 모델이라고 한다. 클레임 기반 모델은 취약점을 신고한 사람이 해당 취약점을 취약점으로 간주할지를 결정할 수 있는 모델이며, 정책 기반 모델은 CNA가 시간을 들여 사실을 정확히 파악하고 정책 기반으로

할당할 수 있는 경우에 사용하는 모델이다.

세 번째 규칙(CNT3)은 취약점에 영향을 받는 구체적인 제품을 식별하는 것이다. 여기서 제품이라는 것은 소프트웨어(상용 및 오픈 소스), 하드웨어, 클라우드 및 소프트웨어 서비스 제공, 프로토콜, 표준 등과 같은 다양한 요소를 포함하는 넓은 의미로 사용된다.

2.2 Inclusion Decision

① INC1: 취약점 보고서가 CNA의 권한 범위 내에 있는지 확인하는 것으로 CNA는 자신의 권한 범위에 따라 정의된 취약점에 대해서만 CVE ID를 할당할 수 있다. 이 권한 범위는 해당 CNA의 최상위 Root CNA에 의해 정의된다.

② INC2: 취약점 보고서 또는 해당 문제가 현재 공개적으로 게시되었거나 앞으로 공개적으로 이용 가능한 장소에 게시되어야 한다. CVE ID는 공개 정보로 사용되며 비공개로 인정되는 취약점에는 할당되지 않는다.

③ INC3: 설치할 수 있거나 고객이 제어할 수 있는 소프트웨어인지 확인한다. 해당 취약점이 특정 웹 사이트에만 존재하거나 온라인 서비스 (소프트웨어로 제공되는 서비스)에만 해당하는지, 또는 고객이 완전히 제어하는 호스팅 솔루션을 통해 제공되는지를 판단한다. CVE ID는 고객이 제어하거나 설치할 수 있는 제품에 할당된다.

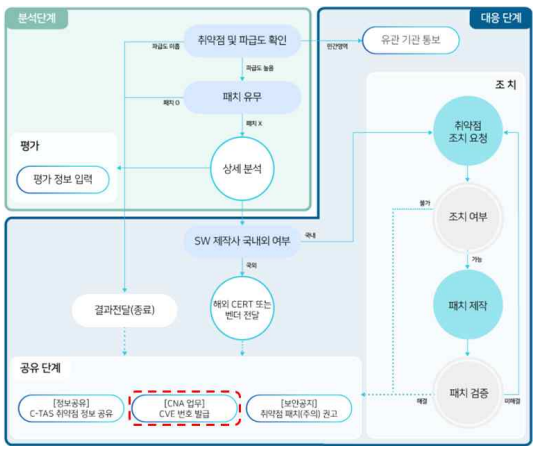
④ INC4: 일반적으로 공개되고 라이선스가 부여된 제품에 영향을 주는 취약점인지 확인한다. 만약 해당 취약점이 발행자나 공급업체의 고객에게 일반적으로 공개되지 않은 소프트웨어 버전에만 영향을 미친다면, 해당 버그에 CVE ID를 할당하지 않는다.

⑤ INC5: 해당 취약점이 이미 CVE로 할당되었거나 CVE 목록에 이미 존재하는지를 확인한다.

CVE ID가 부여되기 위해서는 Counting Decision 3가지와 Inclusion Decision 5가지 조건을 만족해야 한다. 그러나 클라우드 서비스의 경우에는 이러한 규칙 때문에 어려운 상황이 발생하게 되었다. INC3의 규칙이 고객이 통제하지 않거나 CSP가 함께 통제하는 시스템 내 취약점에는 CVE ID를 지정할 수 없게 되어 있기 때문이다. 따라서 이러한 문제점으로 인해 클라우드 서비스에 대한 다양한 취약점 해결책, 영향받은 버전, 참조, 패치와 관련된 정보 등이 CVE 시스템을 통해 공유되지 못하는 결과를 낳게 되어 이에 대한 개선이 필요한 상황이다.

Ⅲ. 클라우드 취약점 제공을 위한 CVE 개선 방안

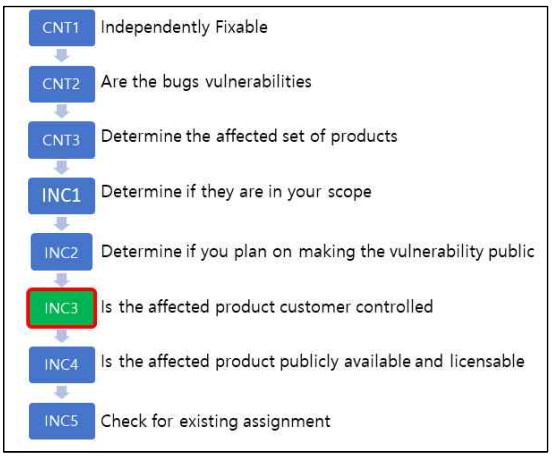
일반적으로 취약점에 대한 대응은 입수단계, 분석단계, 대응단계, 공유단계로 나누어 볼 수 있다[13]. 여기서 입수단계에서는 내부 입수, 신고포상제, 유관기간, 외부신고 등으로부터 취약점을 접수하는 단계이다.



<그림 1> 취약점 공유 절차

<그림 1>과 같이 분석단계에서는 취약점을 분석하

고 파급도를 분석하는 단계이다. 대응단계는 제조사에 취약점에 대한 조치를 요청하는 단계이며, 마지막 공유단계에서 CVE 번호 발급을 요청하여 다른 조직에서도 동일한 취약점에 대응할 수 있도록 공유를 하게 된다. CVE ID가 발급되는 절차는 다음의 <그림 2>와 같다.



<그림 2> CVE ID 발급 절차

여기서 INC3 규칙에 의해 CVE ID 할당을 최종 사용자가 제어할 수 있는 소프트웨어의 취약점으로 제한하고 있다. 사용자가 제어할 수 있는 소프트웨어란 기기에 설치된 모든 소프트웨어, 사용자의 네트워크에 추가된 하드웨어 및 소프트웨어 그리고 해당 기능을 지원하기 위해 사용된 라이브러리 등을 의미한다.

클라우드 서비스의 온프레미스 버전을 사용하는 경우, 온프레미스 소프트웨어의 업데이트를 담당하는 관리자들과의 커뮤니케이션을 위해 CVE ID를 할당하고 있으나, 온프레미스가 아닌 클라우드 서비스의 경우에는 취약점이 발생하더라도 CVE ID를 할당하지 않는 문제점을 가지고 있다. 이는 온프레미스가 아닌 클라우드 서비스의 경우 취약점을 해결하기 위해서는 발견자와 공급업체 간의 커뮤니케이션이 필요하거나 다른 제3자와의 조정이 필요함에 따라 INC3 규칙을 만족하지 않기 때문이다. 즉, 고객이 통제하지 않거나 CSP가 함께 통제하는 시스템 내 취약점에는 CVE ID를 지정할 수 없는 문제가 발생하게 된다. 이는 클라우드 서비스의 취약점 대응을 위한 다양한 정보들이 공유되지 못하게 되어 클라우드 보안관리에 많은 어려움을 초래하게 되었다.

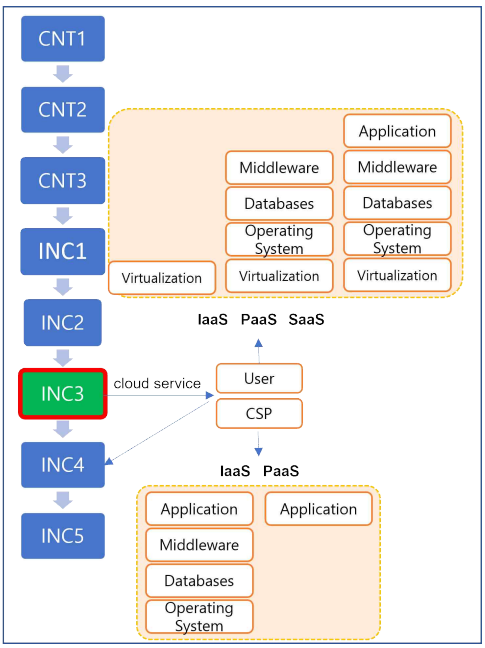
이러한 문제점을 해결하는데 참조할 수 있는 방안으로 클라우드 책임 공유 모델이 있다[14]. 책임 공유 모델은 IaaS, Paas, SaaS 등 클라우드 서비스 제공 형태에 따라 이용자와 클라우드 서비스 제공자의 클라우드 영역별 보안의 책임을 분담하는 것이다. 즉, 영역별로 보안 책임이 누구에게 있는지를 명시하는 것으로 보안에 대한 관리책임을 구체적으로 명시할 수 있다.

온프레미스 버전이 아닌 클라우드 서비스의 경우 CVE ID를 발급받기 위한 전제 조건인 Counting Decision 3가지와 Inclusion Decision 5가지 조건 중 Inclusion Decision의 3번째 조건인 INC3 규칙을 제외한 나머지 조건들은 기본적으로 충족하고 있다. INC3 규칙은 최종 사용자가 제어할 수 있는 소프트웨어의 취약점에 한해 CVE ID를 발급하는 것이므로 이를 클라우드 책임 모델과 매핑하여 고려를 하면 다음의 <표 1>과 같이 각각의 제어 영역을 설정할 수 있다.

<표 1> 클라우드 서비스 주체별 제어 영역

Control Entity	IaaS	PaaS	SaaS
User	Application Middleware Databases OS	Application	
CSP	Virtualization	Middleware Databases OS Virtualization	Application Middleware Databases OS Virtualization

서비스 형태에 따라 사용자와 CSP가 보안 책임을 맡고 있는 각 영역을 설정할 수 있으며, 이에 따라 그 영역에 대한 제어권을 부여할 수 있으므로 클라우드 서비스의 CVE ID 발급을 제한하는 INC3의 제어권 문제를 해결할 수 있다.



<그림 3> INC3 클라우드 서비스 처리 절차

위의 <그림 3>은 INC3 단계에서 클라우드 서비스에 대한 처리 방식을 나타낸 것이다. 이러한 방식은 AWS, 애저, 구글 클라우드 플랫폼 등 다양한 클라우드 서비스플랫폼에도 적용이 가능하다.

여기에서 추가로 고려해야 할 사항으로는 동일한 클라우드 서비스 취약점에 대한 CVE ID의 중복 발급의 가능성이 있다는 것이다. 즉, 동일한 클라우드 플랫폼의 동일한 영역에서 서비스의 형태에 따라 제어하는 주체가 사용자 혹은 CSP로 변경될 수 있기 때문이다. 그러나 이 문제는 INC5 규칙에 의해 해결될 수 있으며, INC5 규칙은 해당 취약점이 이미 CVE로 할당되었거나 CVE 목록에 이미 존재하는지를 확인하기 때문에 이러한 CVE ID 중복 발급 문제를 해결할 수 있다.

보안에서 해킹 공격이 발생하기 위해서는 취약점과 그 취약점을 이용하는 위협이 만나야 공격이 발생하므로 초기에 취약점을 파악하고 이를 공유하여 빠른 대응을 할 수 있게 하는 CVE의 정보 공유는 보안에서 중요한 역할을 담당하고 있으며, 요즘 활성화되고 있는 클라우드 서비스의 취약점에 대한 정보도 CVE 시스템을 통해 공유될 수 있는 정책적인 해결방안을 본 연구를 통해 제시하였다.

IV. 결론

클라우드 서비스가 더욱 확대됨에 따라 클라우드 서비스에 대한 보안도 중요한 이슈가 되고 있다. 이에 따라 정부에서는 클라우드 보안인증제를 수행하여 안전한 클라우드 서비스를 위한 보안점검을 수행하고 있지만, 현재에도 다양한 보안 결함 사항들이 발견되고 있고, 여러 클라우드 보안 사건들도 발생하고 있다. 이러한 클라우드 서비스의 보안성 향상을 위해서는 기존에 알려진 자주 발생하는 취약점에 대한 보완조치를 철저히 이행하고, 새롭게 발생되는 보안 취약점을 주기적으로 조사하여, 조기에 발견 및 S/W 업데이트 및 패치 등을 설치하는 관리활동을 수행해야 한다. 특히, 새롭게 발생되는 취약점은 빠르게 파악하고 이를 공유함으로 그 위험성을 크게 줄일 수 있으며, 이를 위해 CVE를 이용하여 취약점에 대한 정보를 공유하고 있다. 그러나 CVE ID가 부여되기 위해서는 Counting Decision 3가지와 Inclusion Decision 5가지 조건을 만족해야 하는데, 클라우드 특수성 때문에 CVE ID를 지정할 수 없는 문제가 발생하고 있다.

본 논문에서는 클라우드 보안성 향상을 위해 CVE

를 활용할 수 있는 방안에 대한 분석을 수행하였다. CVE ID가 발급되기 위해서는 Counting Decision의 3가지 규칙과 Inclusion Decision의 5가지 규칙을 만족해야 한다. 이중 Inclusion Decision의 3번째 규칙인 INC3가 클라우드 서비스 특성과 충돌하는 문제가 발생하게 되어, 다양한 클라우드 취약점들에 대해 CVE ID가 발급되지 못하는 문제점을 가지고 있다. 따라서 이러한 문제점을 해결하기 위한 연구를 수행하였으며, IaaS, PaaS, SaaS 등 클라우드 서비스별 책임 공유 모델을 활용하여 해결책을 제시하였다. INC3는 고객이 통제하지 않거나 CSP가 함께 통제하는 시스템 내 취약점에는 CVE ID를 지정할 수 없도록 되어 있기 때문에 각 서비스 형태에 따른 영역별 통제 역할을 담당하는 담당자를 지정함으로써 이러한 문제를 해결하였다. 이러한 연구는 CVE에 클라우드 서비스에 대한 취약점이 공유되도록 함으로써 클라우드 서비스 보안성 향상에 중요한 기능을 담당할 수 있다.

향후 연구계획으로는 클라우드 취약점 정보를 제공하고 있는 다양한 관리기관과 정보 제공 사이트들에 대한 정보를 CVE 시스템에 통합하는 방안에 관한 연구를 수행할 예정이다. 이를 통해 클라우드 서비스에 대한 공격 위험을 좀 더 효율적으로 관리할 수 있을 것이라 예상된다.

참고문헌

[1] 김태경 · 백남균 · 김정협, “클라우드 환경에서의 가시성 제공 방안 연구,” 디지털산업정보학회 논문지, 제19권, 제1호, 2023, pp.31-42.

[2] 2023년 클라우드 시장 전망. (https://www.bespinglobal.com/cloud-market-forecast_2023/, Access: 2023년 6월 2일)

[3] 김재현 · 박순태 · 이상무 · 김경백, “클라우드 보안인증(CSAP) 평가 분야별 부적합사항 분석,” 한국정보과학회 학술발표논문집, 2022, pp.1297-1299.

[4] 유승호, “클라우드 인프라의 보안 설정 확인 자동화 기법에 관한 연구,” 아주대학교 석사학위논문, 2021.

[5] 이승욱 · 이재우, “STRIDE 위협 모델링에 기반한 클라우드 컴퓨팅의 쿠버네티스(Kubernetes)의 보안 요구사항에 관한 연구,” 한국정보통신학회논문지 제26권, 제7호, 2022, pp.1047~1059.

[6] 유명성 · 김재한 · 신승원, “컨테이너 이미지 보안성 분석에 관한 연구: Docker Hub 이미지를 중심으로,” 한국통신학회논문지, 제47권, 제8호, 2022, pp.1,231-1,243.

[7] http://cwe.mitre.org

[8] https://nvd.nist.gov/vuln-metrics/cvss

[9] https://cve.mitre.org/cve/update_cve_records.html (Access: 2023년 6월 2일)

[10] https://knvd.krcert.or.kr

[11] https://www.itworld.co.kr/tags/176855/%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C%EC%B7%A8%EC%95%BD%EC%A0%90/244285 (Access: 2023년 6월 2일)

[12] https://www.cve.org/ResourcesSupport/Resources

[13] https://knvd.krcert.or.kr/processingProcedures.do

[14] 한국지능정보사회진흥원, 클라우드의 미래모습과 보안, 미래2030 Vol.2, 2020년 12월.

■ 저자소개 ■

김 태 경
(Kim Taekyung)

2017년 9월~현재
명지전문대학 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학교 교수
2005년 8월 성균관대학교
전기전자및컴퓨터공학과(공학박사)

관심분야 : 네트워크 보안, 클라우드 보안,
개인정보보호
E-mail : tkkim@mjc.ac.kr

정 성 민
(Jung Sungmin)

2020년 9월~현재
명지전문대학 교수
2014년 3월~2020년 8월
한국원자력연구원 선임연구원
2014년 2월 성균관대학교
전기전자및컴퓨터공학과(공학박사)

관심분야 : 산업시설보안, 제어시스템보안,
센서네트워크, 클라우드 컴퓨팅
E-mail : smjung@mjc.ac.kr

논문접수일 : 2023년 6월 6일
수정접수일 : 2023년 6월 14일
게재확정일 : 2023년 6월 15일