공급망 보안 강화를 위한 미국의 정책 추진 현황에 관한 연구

안춘모, 유영상
한국전자통신연구원
cmahn@etri.re.kr, heyyoo@etri.re.kr

A Study on the Current Status of U.S. Policy Implementation to Enhance Supply Chain Security

Ahn Choon Mo, Yoo Young Sang
ETRI

요 약

정보통신을 중심으로 한 기술의 발전과 Covid-19 확산으로 사회경제 시스템은 급격한 디지털화를 경험하며, 재택근무, 비대면 경제사회 활동 등을 완성하고 있다. SW의 생산과 소비도 기존 SW 공급망을 혁신시키며, 디지털에 기반한 공급망 구도로 변화되고 있다. 그럼에도 솔라윈즈 해킹, 카세야 랜섬웨어 유포, Apach Log4j 취약점 공격 등 공급망에 대한 공격이 점차 증대하고 있다. 본 고에서는 공급망 보안 강화를 위해 미국이 추진 중인 행정명령을 중심으로 살펴보고자 한다. 미국이 추진한 정책이나 추진 예정인 정책은 국내의 공급망 보안 강화를 위한 다양한 정책적 시사점을 줄 것으로 판단된다.

Ⅰ. 서 론

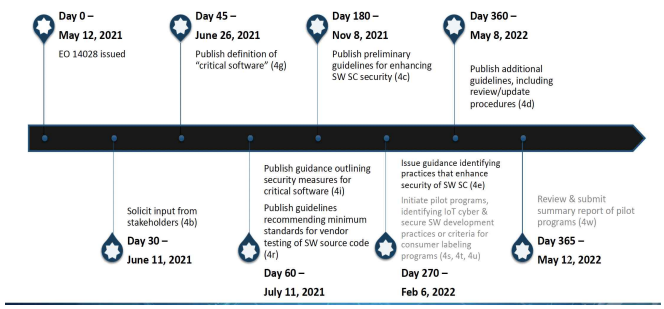
현재의 SW 공급망은 다양한 이해관계자가 연계되어 있기에 공격할 수 있는 공격 표면이 급격히 늘어난 매우 복잡한 구조이다. 가장 아래의 펌웨어 S/W부터 가장 상위에 있는 사용자 서비스 프로그램까지 모두 연결되어 있어 공격자는 중간 단계에 있는 작은 보안취약점 하나만 잘 공략해도 전체 디지털 인프라 위협이 가능하다. 2017년 MeDoc 사건, 2019년 ASUS 공격, 2020년 SolarWinds 사건이 모두 해당되는 사례이다. 또한, 클라우드 환경 구축, 차별화된 원격 기업의 자동 update, 3rd Party의 프로그램 재사용 빈도 증가 등의 보편화에 따라 특정 기업을 공격하면, 해당 기업의 고객이나 자회사 등에도 동시 침투 가능할 정도로 파급성도 높다.

공급망에 대한 위협과 공격은 제품의 생산·유지에 사용되는 SW 내용 및 HW 부품 회로의 구성을 악의적으로 변경하는 범죄 행위로 간주할 수 있다. 더욱기 공급망 공격의 심각성은 단순 금품을 노린 개인의 행위에서 벗어나, 최근에는 국가가 주도하거나 지원하는 전문적인 해킹 그룹이 금전적인 위협뿐 아니라, 국가의 핵심 인프라, 나아가 국가 안보에도 영향을 미치고 있다는 점에 있다.

본 고에서는 공급망 보안 강화를 위한 정책적 노력 관점에서 리딩하고 있는 미국의 사례를 살펴보고자 한다. 2021년 행정명령 EO-14028[1]을 통해 SW의 공급자 뿐만 아니라 수요자에게도 보안 강화를 위해 필수적인 다양한 가이드라인과 핵심 기준 등을 제시했다는 관점에서 매우 의미있는 작업이다. 이를 통해 국내 SW 공급망 보안 강화를 위한 시사점도 논의해 보고자 한다.

Ⅱ. 본론

미국이 공급망 보안 강화를 본격적으로 추진한 시작 시점은 바이든 대통령이 서명하고 2021년 5월 12일 발표된 행정명령 EO-14028, “Executive Order on Improving the Nation’s Cybersecurity”로 평가되고 있다. EO-14028의 주된 지시사항은 중요SW를 정의하고, 연방기관에서 사용하고 있는 중요SW 정보를 취합했으며, 앞으로 연방기관에 납품하는 SW제품에 대해 구성요소 정보를 명기하는 SBOM(Software Bill of Materials) 제출을 의무화하고 있다. 이 가운데 4절에서는 NIST(미국표준기술연구소)가 표준, 절차 및 기준을 참조하여 SW 공급망 보안을 강화하기 위한 관행을 식별하는 다양한 지침을 NIST가 기존 표준, 절차 및 기준을 참조하여 다양한 지침을 게시할 것을 요구하며, 구축 시점에 대해 제시하고 있다. NIST에서 제시한 EO-14028 4절에 대한 업무 및 타임라인은 아래와 같으며, 현재는 대부분 업무가 완료된 것으로 판단된다.



(그림) 행정명령 4절 과업 및 타임라인

* 출처: NIST 홈페이지[2]

위의 그림에서 제시한 일정에 따라 게시된 중요 보고서별 내용은 다음과 같다.

우선적으로 2021년 6월에는 EO-critical SW의 정의를 정하였다[3]. EO-Critical SW는 연방 정부에서 사용하는 주요 SW 제품에 대한 보안 기준을 개발하기 위해 행정명령에서 도입한 개념이다. EO-Critical SW로 지정된 SW에 대해서는 연방 정부가 SW를 구매 및 관리하는 방법을 포함하여 추가적인 활동이 필요하며, 기업은 보안 조치 적용 필요함을 지적하고 있다.

동년 7월에는 critical software의 보안 정도(security measure)를 정리한 지침(guidance)을 제출하였다[4]. 본 지침의 관점은 연방정부가 EO-critical SW를 사용하는 것에 맞추어져 있으며, 개발과 구입(Development & Acquisition)은 논의에서 제외하였다. NIST는 본

security measure에 대한 5개의 목적과 총 20개의 Security Measure를 제시하였다. 지침의 목적은 ① 무단 액세스로부터 보호, ② 데이터 보호, ③ SW 악용 금지, ④ 위협 및 사고 신속 감지, 대응, 복구, ⑤ 인간 행동에 대한 이해와 강화 등에 있으며, 각 목적에 따라 중요 SW 및 중요 SW 플랫폼 보안 조치(Measure)에 대해 제안하였다.

동년 7월 NISTIR 8397 가이드라인을 게시하였다[5]. 본 가이드라인은 공급업체의 소스코드 테스트에 대한 지침 게시를 지시하고 있으며, 이에 따라 NIST는 SW 공급업체 또는 개발자 검증을 위한 최소 표준을 권장하는 문서를 개발하였다. 본 가이드라인에는 벤더나 개발자에 의한 SW 검증 시에 추천되는 11개의 최저 기준 제시하고 있다. 최저 기준은 실행 가능한 컴퓨터 프로그램 전부가 추천되며, 장기적으로는 SW 벤더나 개발자에 대한 강제 기준의 기초가 될 수 있는 것이 명기되어 있다. 본 지침(guidance)에서는 코드 검증을 위해 큰 범주로 ① 위협모델링, ② 정적 및 동적 분석을 위한 자동화 테스트, ③ 정적 (코드-기반) 분석, ④ 동적 분석 등으로 구성하여 제안하였다.

2021년 9월에는 안전한 SW 개발 프레임워크(SSDF version 1.1) 초안이 발표되었으며, 2022년 2월 최종본이 채택되었다[6]. EO-14028 섹션 4e에는 10개의 하위 섹션 또는 항목을 포함하며, 각각은 COTS(상업용) 제품 공급업체, GOTS(정부 규격) SW 개발자, 계약자 및 기타 맞춤형 SW 개발자와 같은 SW 생산자를 위한 조치 또는 결과를 지정하고 있다. EO-14028이 출시되기 전 NIST는 SW 생산자가 따라야 할 결과 기반 보안 SW 개발 관행과 작업을 정의한 초기 SSDF(Secure Software Development Framework)를 발표하였으며, 섹션 4e 항목의 대부분은 원래 SSDF에서 이미 다루고 있었다. 이후 NIST는 섹션 4e의 모든 항목을 해결하기 위해 SSDF를 개정하여 SP 800-218, SSDF(Secure Software Development Framework) 버전 1.1, 「SW 취약점 위험 완화를 위한 권장사항」을 작성한 것이다. SSDF 버전 1.1은 문서번호 NIST SP 800-218로 발표되었으며, 기존 SSDF version 1.0을 대체 (2022년 2월 3일)하고 있다. SSDF의 실행(Practice)은 조직준비, SW보호, 잘 보안된 SW 생산, 취약점 대응 등 네 가지 그룹으로 구성되어있다.

2022년 5월에는 NIST SP 800-161 Rev. 1, Cyber Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations이 게시되었다[7]. 본 문서의 목적은 공급망 전반에 걸쳐 사이버 보안 위험을 관리하는 데 도움이 되도록 기업 전반에 걸쳐 위험 관리 프로세스를 식별, 평가, 선택 및 구현하고 통제를 완화하는 방법에 대한 지침을 기업에 제공하는 것이다. 이때, C-SCRM(사이버 보안 공급망 위험 관리) 전략 구현 계획, C-SCRM 정책, C-SCRM 개발에 대한 지침을 포함하여 다단계, C-SCRM별 접근 방식을 적용하여 C-SCRM를 위험 관리 활동에 통합하고 있다.

마지막으로 2024년 3월에는 Secure Software Development Attestation Form을 게시하였다[8]. EO-14028과 OMB M-22-18 '안전한 소프트웨어 개발 관행을 통한 SW 공급망 보안 강화', OMB M-23-16 'M-22-18 메모랜덤 업데이트'는 연방정부를 위해 일하는 SW 제작업체가 특정 보안 관행을 이행했음을 확인하는 증명 양식의 개발을 요구하였다. 이를 위해 CISA는 이 양식을 예산관리실(OMB)과 긴밀히 협의하고 국가표준기술연구소의 Secure Software Development Framework(SSDF)에 근거하여 개발하였다. 이 안전한 SW 개발 증명 양식의 발표는 CISA, 연방정부 파트너, 국제 동맹국이 추진한 안전한 설계 원칙을 강화할 것으로 기대된다.

Ⅲ. 결론

본 고에서는 SW 공급망 강화를 위한 미국의 행정명령 이행 과정을 중심으로 살펴보았다. 현재 자체 증명 양식 마련을 마지막으로 미국의 SW 공급망 강화를 위한 EO-14028의 이행은 거의 마무리된 것으로 판단된다. 미국은 SW 공급망 위협을 최소화하기 위해 연방정부가 SW공급 업체에 대한 가이드라인 뿐만 아니라, 구매하는 정부부처 측면에서도 행동 양식을 제공하는 적극적인 행정을 진행하고 있다.

현재 국내에서도 물론 ICT 공급망 강화를 위한 시범사업 운영, 유관 기술개발, 도메인별 독자적인 지침도 마련하고 있다. 국내에서도 미국의 사례를 벤치마킹하여 다양한 정책적인 접근을 시도하면서도, 한국의 산업구조에 차별화되고 적합한 정책의 발굴도 진행될 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 한국전자통신연구원 연구운영지원사업의 일환으로 수행되었음 [24ZF1100, 국가 지능화 기술정책 및 표준화 연구].

참 고 문 헌

[1] The White House, Executive Order 14028: Improving the Nation's Cybersecurity, 2021. 5. 12.

[2] NIST 홈페이지, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[3] NIST, Definition of Critical Software Under Executive Order (EO) 14028, 2021. 10. 13.

[4] NIST, Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, 2021. 7. 9.

[5] NIST, Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028, 2021. 7. 7.

[6] NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, 2022. 2.

[7] NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 2022. 5.

[8] CISA, Secure Software Development Attestation Form, 2024. 3. 18.