OpenChain 보안 보증

참고 가이드

Version 1.0

*소프트웨어 솔루션을 구성하는 오픈소스에 대한 신뢰 구축*

Contents

[소개 iii](#_Toc83652366)

[1 적용 범위 1](#_Toc83652367)

[2 용어와 정의 1](#_Toc83652368)

[3 요구사항 2](#_Toc83652369)

[3.1 프로그램 설립 2](#_Toc83652370)

[3.1.1 정책 2](#_Toc83652371)

[3.1.2 역량Competence 2](#_Toc83652372)

[3.1.3 인식 3](#_Toc83652373)

[3.1.4 프로그램 적용 범우 3](#_Toc83652374)

[3.1.5 표준 업무 사례 구추 4](#_Toc83652375)

[3.2 관련 업무 정의 및 지원 4](#_Toc83652376)

[3.2.1 외부 문의 대응 (Access) 4](#_Toc83652377)

[3.2.2 효과적인 리소스 제공 5](#_Toc83652378)

[3.3 오픈 소스 콘텐츠 검토 및 승인 5](#_Toc83652379)

[3.3.1 BOM (Bill of Materials) 5](#_Toc83652380)

[3.3.2 보안 보증 6](#_Toc83652381)

[3.4 가이드 요구사항 준수 6](#_Toc83652382)

[3.4.1 완성도 6](#_Toc83652383)

[3.4.2 지속 기간 7](#_Toc83652384)

소개

OpenChain Specification 워킹 그룹의 핵심 역할은 현대의 소프트웨어 솔루션을 개발하는데 있어서 오픈소스에 대한 신뢰를 확립하는 프로그램 표준을 개발하는 것이다. OpenChain 프로젝트의 대표 규격인 ISO 5230 국제 표준은 현재 오픈소스 라이선스 컴플라이언스를 중심으로 신뢰를 구축하는데 중점을 두고 있다. 보다 넓은 범위의 역할을 지원하기 위한 다음 단계는 오픈소스 사용과 관련하여 모든 보안 보증 프로그램이 충족해야 할 최소 핵심 요구 사항을 식별하고 제시하는 가이드를 개발하는 것이었다. 우선 오픈소스에서 알려진 공개 보안 취약점 문제(예: CVE, GitHub/GitLab 취약점 경고, 패키지 관리자 경고 등)가 있는지 확인하는 것으로 범위를 한정한다. 이러한 가이드의 범위는 시간이 지남에 따라 커뮤니티 피드백을 반영하여 확장할 수 있다.

이 참조 가이드를 준수한다는 것은 조직이 사용하는 오픈소스와 관련하여 신뢰할 수 있는 수준의 보안 보증Security Assurance을 구축하기 위해 필요한 단계를 수행하는 프로그램을 갖추었음을 보증한다. 이 문서는 프로그램의 "How"와 "When"보다는 "What"과 "Why" 측면에 중점을 둔다. 이를 통해 다양한 산업에서 각기 다른 조직의 규모, 목표, 프로그램 범위에 맞는 구체적인 정책과 프로세스 콘텐츠를 선택할 수 있는 유연성을 보장한다. 예를 들어, OpenChain 적합 프로그램은 단일 제품군 또는 전체 조직을 대상으로 적용할 수 있다.

이 소개에서는 가이드의 목적을 설명한다. 2장에서는 이 문서 전체에서 사용되는 주요 용어를 정의한다. 3장에서는 프로그램이 핵심 수준의 보안 보증을 달성하기 위해 충족해야 하는 요구 사항을 정의한다. 각 요구 사항은 이를 충족하기 위해 생성해야 하는 하나 이상의 입증 자료(문서 등)를 포함한다. 입증 자료를 공개해야 하는 것은 아니지만, 필요할 경우 NDA(Non-Disclosure Agreement)를 맺고 다른 조직에 제공할 수 있다.

이 참고 가이드는 [Creative Commons Attribution License 4.0](https://creativecommons.org/licenses/by/4.0/) (CC-BY-4.0)에 따라 라이선스가 부여된다.

OpenChain 보안 보증 참고 가이드

# 적용 범위

이 문서는 오픈소스로 구성된 소프트웨어 솔루션을 주고 받는 조직 간에 신뢰를 구축하기 위한 우수한 오픈소스 보안 보증 프로그램의 핵심 요구사항을 정의한다.

# 용어와 정의

이 문서의 목적을 위해 다음과 같은 용어와 정의를 적용한다.

**2.1 CVE**

CVE(Common Vulnerability and Exposure)는 발견된 컴퓨터 소프트웨어 보안 문제 및 결함에 대한 공개 데이터베이스이다. 누군가 CVE를 언급한다면 데이터베이스 내에서 CVE ID 번호가 할당된 보안 결함을 의미한다. CVE 데이터베이스는 미국 국토 안보부US Department of Homeland Security (DHS)와 사이버 보안 및 인프라 보안국Cybersecurity and Infrastructure Security Agency (CISA)이 후원한다.

**2.2** **알려진 취약점**

공개적으로 사용 가능한 오픈소스 컴포넌트에서 발견된 보안 취약점을 의미한다. 여기에는 CVE, GitHub/GitLab 취약점 경고, 패키지 관리자 경고 등을 포함하되 이에 국한되지 않으며 공개적으로 게시된 취약점이 포함된다.

**2.3 오픈소스**

Open Source Initiative에서 만든 Open Source Definition (opensource.org/osd) 혹은 Free Software Foundation에서 만든 Free Software Definition (gnu.org/philosophy/free-sw.html)을 충족하는 라이선스, 혹은 이와 유사한 라이선스가 하나 이상 적용된 소프트웨어이다.

**2.4 프로그램**조직의 보안 보증 활동을 구성하는 정책, 프로세스 및 인력의 집합

**2.5 프로그램 참여자**배포용 소프트웨어를 만들고, 이에 기여하거나 준비할 책임이 있는 모든 조직 구성원 혹은 계약자

참고: 조직에 따라 소프트웨어 개발자, 릴리스 엔지니어, 품질 엔지니어, 제품 마케팅 및 제품 관리자가 포함될 수 있다(단, 이에 국한되지는 않는다).

**2.6 보안 보증**시스템이 보안 모범 사례에 대한 요구 사항을 충족하고 알려진 취약점에 대한 대응력을 갖추고 있다는 확신

**2.7 SPDX**소프트웨어 패키지를 주고 받을 때 라이선스, 저작권 정보 및 알려진 취약점을 포함한 BOM(Bill of Materials)을 교환하기 위해 Linux Fouindation의 SPDX(Software Package Data Exchange) Working Group에서 만든 형식 표준(spdx.org 참조)

**2.8 배포용 소프트웨어**조직이 제 3자(예: 다른 조직 또는 개인)에게 배포하거나 제공하는 소프트웨어

**2.9 입증 자료**이 참고 가이드의 요구사항이 충족되었음을 입증하는 자료

# 요구사항

## 프로그램 설립

### 정책

배포용 소프트웨어의 오픈소스 보안 보증을 관리하는 문서화된 오픈소스 정책이 있어야 한다. 이 정책은 조직 내부에 전파되어야 한다.

**입증 자료:**

* 3.1.1.1 문서화된 오픈소스 보안 보증 정책
* 3.1.1.2 프로그램 참여자가 오픈소스 보안 보증 정책의 존재를 알 수 있게 하는 문서화 된 절차 (교육, 내부 위키, 혹은 기타 실질적인 전달 방법 등).

**이유:**

오픈소스 보안 보증 정책을 만들고, 프로그램 참여자가 이 정책의 존재를 인식하도록 보장하기 위해서이다. 정책에 어떤 사항이 포함되어야 하는 지에 대해서는 다음 섹션에서 다룬다.

### 역량

조직은 다음 사항을 수행해야 한다.

* 프로그램의 성과와 효율에 영향을 미치는 역할이 무엇인지, 그 역할에 해당하는 책임은 무엇인지 확인한다.
* 각 역할을 수행할 프로그램 참여자가 갖춰야 할 필요 역량을 결정한다.
* 프로그램 참여자가 적절한 교육, 훈련 및/또는 경험을 바탕으로 자격을 갖춘 자임을 확인한다.
* 해당되는 경우, 필요한 역량을 확보하기 위해 조치한다.
* 역량 보유를 증명하기 위한 정보를 문서화하여 유지한다.

**입증 자료:**

* 3.1.2.1 프로그램의 여러 참여자에 대한 역할과 각 역할의 책임을 나열한 문서
* 3.1.2.2 각 역할을 위해 필요한 역량을 기술한 문서
* 3.1.2.3 각 프로그램 참여자의 역량을 평가한 문서화된 증거

**이유:**

프로그램 참여자가 각자의 역할과 책임을 위한 충분한 수준의 역량을 확보하였음을 보장하기 위해서이다.

### 인식

조직은 프로그램 참여자가 다음 사항을 인식하도록 보장해야 한다:

* 오픈소스 보안 보증 정책
* 관련 프로그램 목표
* 효과적인 프로그램이 되기 위한 참여자의 기여 방법
* 프로그램 요구사항을 준수하지 않을 경우 미치는 영향

**입증 자료:**

* 3.1.3.1 다음 사항에 대한 프로그램 참여자의 인식을 평가하였음을 나타내는 문서화된 증거 : 프로그램의 목표, 프로그램 내에서의 참여자 기여 방법 및 프로그램을 준수하지 않을 경우 미치는 영향

**이유:**

프로그램 참여자가 프로그램 내에서 각자의 역할과 책임에 대해 충분한 수준의 인식을 갖고 있음을 보장하기 위해서이다.

### 프로그램 적용 범위

프로그램은 다양한 범위 별로 적용하여 관리할 수 있다. 예를 들어, 한 프로그램을 단일 제품군에만 적용할 수도 있고, 전체 부서 또는 전체 조직에 적용하여 관리할 수 있다. 따라서 각 프로그램에서는 적용 범위를 정확히 명시해야 한다.

**입증 자료:**

* 3.1.4.1 프로그램의 적용 범위와 한계를 명확하게 정의한 문서화된 진술

**이유:**

조직의 필요 범위에 맞게 가장 적합한 프로그램을 유연하게 구성하기 위해서이다. 어떤 조직은 프로그램을 특정 제품군을 관리하도록 적용할 수 있고, 또 어떤 프로그램은 전체 조직에서 배포하는 소프트웨어를 관리하도록 지정할 수 있다.

### 표준 업무 사례 구축

* 조직이 알려진 취약점에 대한 지식을 갖고 있음
* 배포용 소프트웨어에 대해 알려진 취약점의 존재를 탐지하는 방법
* 식별된 알려진 취약점에 대한 후속 조치 방법
* 식별된 알려진 취약점을 보증이 필요한 고객에게 전달하는 방법Method to communicate identified Known Vulnerabilities to customer base when warranted
* 배포 후 새로 게시된 알려진 취약점에 대하여 배포용 소프트웨어를 분석을 위한 방법

위와 같은 보안 보증 방법을 위한 프로세스가 존재해야 한다.

**입증 자료:**

* 3.1.5.1 위에서 설명한 각 방법에 대한 문서화된 절차가 있어야 한다.

**이유:**

배포용 소프트웨어에서의 알려진 취약점을 감지하고 후속 조치를 취하기 위한 적절한 프로세스가 있음을 보장하기 위해서이다.

## 관련 업무 정의 및 지원

### 외부 문의 대응 (Access)

외부로 부터의 알려진 취약점 문의에 효과적으로 대응하기 위한 프로세스를 유지해야한다. 제 3자가 특정 소프트웨어 제품과 관련하여 알려진 취약점에 대해 문의 할 수 있는 방법을 공개해야 한다.

**입증 자료:**

* 3.2.1.1 제 3자가 알려진 취약점에 대해 문의 할 수 있는 공개된 방법 (예: 공개된 담당자 이메일 주소 - security@company.com, opensource@company.com, …)
* 3.2.1.2 제 3자의 알려진 취약점 문의에 대응하기 위한 내부의 문서화된 절차가 있어야 한다.

**이유:**

제 3자가 보안 취약점 문의를 위해 조직에 연락할 수 있는 합리적인 방법을 제공하고, 조직이 이를 효과적으로 대응할 수 있는 준비가 되어 있는지 보장하기 위해서이다.

### 효과적인 리소스 제공

프로그램이 효과적일 수 있도록 다음과 같이 업무를 정의하고 리소스를 제공해야 한다:

* 프로그램을 성공적으로 수행할 수 있도록 각 업무에 대한 책임을 할당한다.
* 프로그램의 업무를 위한 충분한 리소스를 제공한다.
  + 충분한 업무 수행 시간을 할당한다.
  + 예산을 적절하게 지원한다.
* 정책 및 지원 업무를 검토하고 개선하는 프로세스가 존재한다.
* 알려진 취약점과 관련된 기술 전문 지식을 가이드가 필요한 사용자에게 제공한다.

**입증 자료:**

* 3.2.2.1 프로그램 내 각 역할을 담당하는 인원, 그룹 또는 직무의 이름을 기재한 문서
* 3.2.2.2 프로그램 내 각 역할을 담당하는 인원이 적합하게 배치되고, 예산이 적절하게 지원되어야 한다.
* 3.2.2.3 식별된 알려진 취약점을 해결하는데 사용할 수 있는 전문 지식 활용 방법
* 3.2.2.4 보안 보증에 대한 내부 책임을 할당하는 문서화된 절차
* 3.2.2.5 식별된 알려진 취약점 사례를 검토하고 이를 수정하기 위한 문서화된 절차

**이유:**

i) 프로그램 내 각 역할을 효과적으로 지원하며 리소스를 제공하고, ii) 정책 및 지원 프로세스가 보안 보증 모범 사례의 변경 사항을 수용하도록 정기적으로 업데이트되고 있음을 보장하기 위해서이다.

## 오픈 소스 콘텐츠 검토 및 승인

### BOM (Bill of Materials)

배포용 소프트웨어를 구성하는 오픈소스 컴포넌트에 대한 BOM(Bill of Materials)을 생성하고 관리하는 프로세스가 있어야 한다.

**입증 자료:**

* 3.3.1.1 배포용 소프트웨어를 구성하는 오픈소스 컴포넌트에 대한 정보를 식별, 추적, 검토, 승인 및 보관하는 문서화된 절차
* 3.3.1.2 문서화된 절차가 적절히 준수되었음을 보여주는 배포용 소프트웨어에 대한 오픈소스 컴포넌트 기록

**이유:**

배포용 소프트웨어를 구성하는데 사용되는 오픈소스 컴포넌트 BOM을 생성하고 관리하기 위한 프로세스가 있음을 보장하기 위해서이다. 각 컴포넌트에 알려진 취약점이 존재하는지 체계적으로 검토하기 위해서는 BOM이 필요하다.

### 보안 보증

* 검토 중인 배포용 소프트웨어 릴리스에 대한 BOM (Bill of Materials)의 각 오픈소스 컴포넌트에 대해
  + 알려진 취약점이 존재하는지 검출할 수 있는 방법을 적용한다.
  + 식별된 각 알려진 취약점에 대해 위험도/영향도 점수를 할당한다.
  + 위험도/영향도 점수에 따라 적절한 조치를 취한다(예: 보증이 필요한 고객에게 연락, 컴포넌트 업그레이드, 추가 조치 없음 등).
  + 이전에 배포한 배포용 소프트웨어에 알려진 취약점이 있는 경우, 위험도/영향도 점수에 따라 적절한 조치를 취한다(예: 보증이 필요한 고객에게 연락).
* 소프트웨어 솔루션 출시 후 활동 - 추후 새롭게 보고된 알려진 취약점 중 배포용 소프트웨어 솔루션에 영향을 미칠 수 있는 취약점을 식별하고 그에 따라 대응할 수 있는 능력이 있어야 한다.

**입증 자료:**

* 3.3.2.1 배포용 소프트웨어의 오픈소스 컴포넌트에 대해 알려진 취약점을 탐지하고 해결하기 위한 문서화된 절차
* 3.3.2.2 각 오픈소스 컴포넌트에 대해 식별된 알려진 취약점 및 취한 조치(조치할 필요가 없는 경우도 포함)에 대한 기록을 유지한다.

**이유:**

프로그램이 배포용 소프트웨어를 구성하는 오픈소스에 대해 식별된 알려진 취약점을 처리할 수 있을 만큼 충분히 견고하고, 이 활동을 지원하기 위한 절차가 존재하며 이 절차가 준수됨을 보장하기 위해서이다.

## 가이드 요구사항 준수

### 완성도

프로그램이 이 참고 가이드를 준수한다고 간주하기 위해서는 조직은 프로그램이 이 문서에서 제시한 모든 요구사항을 충족하는지 확인해야 한다.

**입증 자료:**

* 3.4.1.1 제3.1.4조에서 명시한 프로그램이 이 문서의 모든 요구사항을 충족함을 확인하는 문서

**이유:**

조직이 이 참고 가이드에 적합한 프로그램을 보유했다고 선언하는 것은 그 프로그램이 이 문서의 모든 요구사항을 충족하고 있음을 보장하기 위해서이다. 이 요구사항의 일부 만을 충족하는 것으로는 충분하지 않다.

### 지속 기간

이 참고 가이드의 버전에 적합한 프로그램은 적합성 인증을 획득한 날로부터 18개월 동안 지속되어야 한다.

**입증 자료:**

* 3.4.2.1 프로그램이 적합성 인증을 획득한 후 지난 18개월 동안 이 가이드의 모든 요구사항을 충족하고 있음을 확인하는 문서

**이유:**

조직이 시간이 지나도 적합성을 주장하고자 한다면 프로그램을 참고 가이드에 맞게 계속 유지하는 것이 중요하다. 이 요구사항은 시간이 지난 후 조직이 계속해서 프로그램 적합성을 주장하더라도 프로그램의 지원 프로세스와 통제가 약화되지 않았음을 보장하기 위해서이다.