Criteria and attestation for maintaining provenance of code and components including open-source software

NIST Executive Order on Cyber Security Workshop
November 8, 2021
Relevant Executive Order Sections

- 4 (e) (vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;
- 4 (e) (vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;
- 4 (e) (x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.
GitHub - microsoft/scim: Supply Chain Integrity Model
Build tool and OSS provenance management today

- Public Package and Image Managers
- User Access Control and Review
- Security Monitoring
- Security Ingestion Gates
- Governance
- Build Agent VM/Containers
- Packages
- Build Definitions
- Repo Clone
- Trusted Build Environment
- Trusted Build Artifact Repositories
- Source Control
- Secure Deployment
- Tooling updates through PR automation
- Build Tools, Compilers, SDKs
- Policy Enforcement Automation

Build tool and OSS provenance management today.
OSS ingestion & provenance

Public Package and Image Managers

Security Ingestion Gates & Governance

Azure Container Registry

Azure Artifacts

Trusted Build Environment

SBOM

Build Output

Policy Enforcement Automation

Secure Deployment

Component Governance

Build Definitions

Packages

Repo Clone

CloudMine → Newtonsoft.Json 13.0.1

Overview

Versions

Connect to feed

Download

Promote

Unlist ...

Provenance

Publisher

using NuGet VS VSIX/5.10.0 (Microsoft Windows NT 10.0.19043.0, Enterprise/16.0)

Jul 1 (7/1/2021 7:26:37 PM)

Description

Json.NET is a popular high-performance JSON framework for .NET

People

Authors

James Newton-King

Development

Source

NuGet Gallery

Project

Homepage

License MIT

automation

Build tools, Compilers, SDKs
Future tool and OSS provenance management

Public Package and Image Managers

Security Ingestion Gates & Governance

Azure Container Registry

Azure Artifacts

Source Control

Build Tooling, Compilers

Trusted Build Artifact Repositories

Component Governance

Trusted Build Environment

Build Agent VM/Containers

Packages

Build Definitions

Repo Clone

Build Artifacts

SBOM Validation

Secure Deployment

User Access Control and Review

Security Monitoring

Security boundary

Tooling updates through PR automation

Policy Enforcement Automation

Product SBOM

Claims

Build Agent SBOM

Evidence

SCIM Ledger

Trusted Build Artifact Repositories
SBOM generation at build time

Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft - Engineering@Microsoft
**Claimant:** Build5

**Subject:** PRD-107217

**Requirement:** EO.14028.Sec4/4(e)(vii)

**Evidence:** SBOM1, SBOM2

---

"Build5"

1. Generates SBOMs
2. Constructs claim

---

**Subject Inventory**
- PRD-107217
- Azure Key Vault

**Requirement Inventory**
- EO.14028.Sec4/4(e)(vii)
  - Provide a purchaser an (SBOM) for each product

---

```
"type": "Document",
"spdxVersion": "3.0-DRAFT",
"elements": []

"type": "Claim",
"claimant": "build5",
"subject": "svk",
"predicate": "https://potomac.microsoft.com/types/predicate/conformance/",
"predicateType": "https://potomac.microsoft.com/types/predicate/conformance/",
"start": "2019-01-02T23:15:00+01:00",
"end": "2020-12-31T23:45:00+01:00",
"evidence": [":sbom1", ":sbom2"]

"id": "svk",
"type": "Package",
"name": "Azure Key Vault",
"externalReferences": ["https://potomac.microsoft.com/collectors/MS.Subjects/PRD-107217/"

"id": "build5",
"type": "Tool",
"name": "Build System 5",
"externalReferences": ["https://potomac.microsoft.com/tool/build/buildsystem5/"

"externalMap": [

"externalID": ":sbom1", "elementURL": "[...]/sbom1.sbn",
"externalID": ":sbom2", "elementURL": "[...]/sbom2.sbn"

```
Thank you

NIST Executive Order on Cyber Security Workshop
November 8, 2021