Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date December 15, 2020

Original Release Date February 10, 2020

Superseding Document

Status	Final
Series/Number	NIST Interagency or Internal Report 8246
Title	Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers
Publication Date	December 2020
DOI	https://doi.org/10.6028/NIST.IR.8246
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8246/final
Additional Information	

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8246

National Vulnerability Database (NVD) Metadata Submission Guidelines for Common Vulnerabilities and Exposures (CVE) Numbering Authorities (CNAs) and Authorized Data Publishers

Robert Byers
David Waltermire
Christopher Turner

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8246-draft

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8246

National Vulnerability Database (NVD) Metadata Submission Guidelines for Common Vulnerabilities and Exposures (CVE) Numbering Authorities (CNAs) and Authorized Data Publishers

Robert Byers
David Waltermire
Computer Security Division
Information Technology Laboratory

Christopher Turner
CocoaSystems Inc
Eldersburg, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8246-draft

February 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8246
30 pages (February 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8246-draft

Public comment period: February 10, 2020 through March 20, 2020

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: NISTIR_8246-Comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The purpose of this document is to leverage the strength of technical knowledge provided by the Common Vulnerabilities and Exposures (CVE) Numbering Authorities (CNAs) and the application of consistent and unbiased CVE metadata provided by the National Vulnerability Database (NVD) analysts through the formalization of a CVE metadata submission process. This process will enable outside entities to submit CVE metadata and allow this data to be presented to the end user with little to no NVD analyst involvement. For instances where the CVE metadata is provided, the NVD analyst will serve in the role of auditor to ensure consistent quality and integrity standards are applied, maintained, and communicated. Public recognition of the upstream participants' level of effort and quality of data will be displayed on the public NVD website's CVE detail page to encourage and incentivize participation.

Keywords

Accreditation Level; Authorized Data Publisher (ADP); Common Vulnerabilities and Exposures (CVE); CVE Numbering Authority (CNA); Submission Category.

Audience

Consumers who might benefit most from this publication include CVE Numbering Authorities, Authorized Data Publishers and downstream consumers of NVD CVE data feeds.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: NISTIR_8246-Comments@nist.gov

Table of Contents

List of Appendices

1 Introduction

The number of Common Vulnerabilities and Exposures identifiers (CVE IDs) created year over year has rapidly increased, and this trend is expected to continue indefinitely. In the past, the CVE program was constrained by the limited resources at the MITRE Corporation (MITRE). Decoupling efforts within MITRE have successfully allowed for the significant increase in CVE submissions by CVE Numbering Authorities (CNAs) seen today and have resulted in a scalable solution to support growth in the CVE program for the foreseeable future. MITRE still maintains an oversight role for CNAs to ensure proper procedures, content quality, and content consistency are maintained within the CVE program. By delegating the publication of CVE entries to CNAs, there is a significant gain in leveraging the knowledge base of the CNAs and distributing the CVE workload across multiple CNA resources. Downstream users are direct beneficiaries of this cooperation as more vulnerabilities are released from a trusted source, improving the security of our national IT infrastructure for both public and private entities.

As a result of MITRE's success in delegating the CVE process to the CNAs, a new resource constraint has been introduced downstream. Currently, the National Vulnerability Database (NVD) Analysts add five types of metadata to each CVE: Common Vulnerability Scoring System (CVSS) version 3.1 (v3.1) scores, CVSS version 2 (v2) scores, Common Weakness Enumerations (CWE), Reference Tags, and Configurations. This is a manual, human resource-intensive process maintained by a government entity. The ability to increase staff indefinitely to support this growth is not sustainable. Today, there are entities that provide some of this basic NVD metadata; however, there are no policies or procedures in place to ensure that metadata provided in CVE entries follows the same consistent criteria applied by the NVD analysts across all CVE entries, regardless of vendor or product.

2 Purpose and Scope

The purpose of this document is to leverage the strength of technical knowledge provided by the CNAs and the application of consistent and unbiased CVE metadata provided by the NVD analysts through the formalization of a CVE entry metadata submission process. This process will enable outside entities to submit CVE entry metadata and allow this data to be presented to the end user with little to no NVD analyst involvement. For instances where the CVE entry metadata is provided, the NVD analyst will serve in the role of auditor to ensure consistent quality and integrity standards are applied, maintained, and communicated. Public recognition of the upstream participants' level of effort and quality of data will be displayed on the CVE detail page within the public NVD website to encourage and incentivize participation. Although many CVE entries received by the NVD will not provide this metadata, there are many entities that have the interest and expertise to do so. Although it is difficult to predict actual CVE growth and the participation levels of the submission process, it is expected that once this process is in place and adopted, it will provide some relief to the continuously growing workload faced by the NVD.

3 Roles and Responsibilities

This section identifies the roles and responsibilities for entities providing CVE entry metadata.

Table 1: CVE Entry Metadata Contribution Roles and Responsibilities

NVD Analyst	The NVD staff responsible for the entry and oversight of the CVE entry metadata created by the NVD
CVE Numbering Authority (CNA)	The entity authorized to assign CVE IDs to products within a distinct authorized scope. This scope is defined within the CNA Charter, and the NVD will rely on the CNA program to ensure assignments were made within a CNA's appropriate scope.
Authorized Data Publisher	The entity providing additional data related to a previously populated CVE entry within a distinct, agreed-upon scope

4 Current NVD Analyst Workflow

The current NVD analyst workflow for a single CVE entry consists of two primary stages: Initial Analysis and Verification. Initial Analysis involves an NVD analyst investigating the information provided for the CVE entry to better understand the vulnerability's characteristics. This analysis is primarily focused on the CVE description and attached resource links to external publicly verifiable information. From this information, the NVD analyst develops initial CVSS v3.1 and CVSS v2 vector strings, associates CWE(s) with the CVE, determines the appropriate Reference Link Tags, and builds the configurations using match criteria as defined in the Common Platform Enumeration (CPE) 2.3 specification.

Once the Initial Analysis is complete, the analyzed metadata for the CVE entry is then reviewed by a second—usually more experienced—NVD analyst during the Verification stage. This ensures the proper standards and procedures have been applied to the analysis of CVE metadata based on the information supplied. Once the CVE has been reviewed, the CVE metadata is then published for public access.

5 External Submission Workflow

The External Submission process for both the CNA and the Authorized Data Publisher begins by editing the CVE JSON file as noted in Appendices C, D, E, and F and following the approval process defined by MITRE (https://cve.mitre.org/cve/cna.html). This process is the only mechanism in place for providing CVE Entry metadata. CNAs and Authorized Data Publishers will not have direct access to the NVD administrative site. Once the content has been submitted, the workflow for CNAs will be dependent on the type of CVE metadata (referred to as Submission Categories) provided and the Acceptance Level achieved. Specific details on this process and the Acceptance Level criteria are further defined below. The content submitted by an Authorized Data Publisher is utilized by the NVD analyst as reference data and displayed on the public NVD website.

Additional details are provided in the Submission Categories and Acceptance Levels sections later in this document.

6 Submission Categories

There are five Submission Categories that can be provided within the CVE JSON file. There are no dependencies between the Submission Categories, and each Submission Category is optional. Both CNAs and Authorized Data Publishers may choose which Submission Categories to contribute. The categories, each of which is discussed in more detail later in this section, are as follows:

- CVSS v3.1 Base Metric Group
- CVSS v2 Base Metric Group
- CWEs
- Reference Link Tags
- Configurations

6.1 CVSS v3.1 Base Metric Group

The CVSS v3.1 Base Metric Group consists of eight metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality Impact, Integrity Impact, and Availability Impact. Values selected for each of these metrics are used to compute the CVSS v3.1 Base Metric score. See the CVSS v3.1 Specification Document[1] for more detailed information. See Appendix C for accepted JSON schema and sample data.

6.2 CVSS v2 Base Metric Group

The CVSS v2 Base Metric Group consists of six metrics: Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact, and Availability Impact. Values selected for each of these metrics are used to compute the CVSS v2 Base Metric score. See the CVSS Version 2.0 guide[2] [3] for more detailed information. See Appendix D for accepted JSON schema and sample data.

6.3 CWE

CWE is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and a baseline for weakness identification, mitigation, and prevention efforts. See the CWE home page[4] for more detailed information on CWE. See Appendix E for accepted JSON schema and sample data.

---

1 FIRST (2019) *Common Vulnerability Scoring System v3.1: Specification Document*. Available at https://www.first.org/cvss/specification-document.

2 Mell P, Scarfone K, Romanosky S (2007) *CVSS: A Complete Guide to the Common Vulnerability Scoring System, Version 2.0*. Available at https://www.first.org/cvss/v2/guide.

3 Mell P, Scarfone K, Romanosky S (2007) *The Common Vulnerability Scoring System (CVSS) and its Applicability to Federal Agency Systems*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7435. https://doi.org/10.6028/NIST.IR.7435

4 https://cwe.mitre.org/

6.4 Reference Link Tags

The Reference Link Tags support the categorization of each reference attached to the CVE. This categorization allows the end user to quickly identify relevant reference links. Table 2 contains the valid Reference Link Tag Values.

Table 2: Valid Reference Link Tag Values

Reference Link Tag Value	Description
U.S. Government Resource	The reference link is from a U.S. Government agency or organization (.mil or .gov).
VDB Entry	Vulnerability databases (VDBs) are loosely defined as sites that provide vulnerability information, such as advisories, with identifiers. Included VDBs are free to access, substantially public, and have broad scope and coverage (not limited to a single vendor or research organization). See: https://www.first.org/global/sigs/vrdx/vdb-catalog
Vendor Advisory	The advisory is from the vendor/publisher of the product or the parent company that owns the vendor.
Third-Party Advisory	The advisory is from an organization that is not the vulnerable product's vendor or publisher (or the vendor or publisher's parent company).
Patch	The reference contains an update to the software that fixes the vulnerability.
Mitigation	The reference contains information on steps to mitigate the vulnerability in the event a patch cannot be applied or is unavailable.
Exploit	The reference contains an in-depth, detailed description of steps to exploit a vulnerability or any legitimate POC code or exploit kit.
Press/Media Coverage	The reference is from a media outlet such as a newspaper, magazine, social media, or web log. This tag is not intended to apply to any individual's personal social media account. It is strictly intended for public media entities.
Issue Tracking	The reference is a post from a bug tracking tool.
Mailing List	The reference is from a mailing list, often specific to a product or vendor.
Release Notes	The reference is in the format of a vendor or open-source project's release notes or change log.
Technical Description	The reference contains in-depth technical information about a vulnerability and its exploitation process. It can be in the form of a presentation or white paper.

Reference Link Tag Value	Description
Product	The reference is appropriate for describing a product for the purposes of a CPE ID or a Software Identification (SWID) Tag.
Permissions Required	The reference link provided is blocked by a login page. If credentials are required to see any information, this tag must be applied.

See Appendix F for accepted JSON schema and sample data.

6.5 Configurations

Configurations within the NVD consist of two primary items: the CPE match string and the CPE. The overall purpose of the configuration is to provide a flexible mechanism to express the products impacted by the CVE. See the NVD's Known Affected Software Configurations[5] for more detailed information on Configurations. See Appendix G for accepted JSON schema and sample data.

[5] https://nvd.nist.gov/vuln/vulnerability-detail-pages

7 Acceptance Levels

For each of the Submission Categories selected by the CNA, an Acceptance Level will be assigned. The possible Acceptance Levels, each of which are discussed in more detail below, are:

- Non-Acceptance
- Reference
- Contributor
- Provider

7.1 Non-Acceptance

Non-Acceptance is used when the CNA's content has been deemed unfit for display on the NVD website or for inclusion within the NVD data feeds (i.e., content contains classified, offensive, or derogatory content).

7.2 Reference

Reference is the starting Acceptance Level for all Submission Categories and CNAs. The CNA will receive public acknowledgement on the CVE detail page of the NVD website. If the Submission Category content matches what the NVD analyst has provided, the content will be shown as a single row and the CNA acknowledged as the source with NVD verification. If the CAN content does not match the NVD analyst content, the content will be shown separately for the NVD analyst and the CNA. Only the NVD analyst information will be available in the data feeds and web service content.

Authorized Data Publishers are only assigned an Acceptance Level of Reference or Non-Acceptance. CVE entry metadata provided by Authorized Data Publishers will not be evaluated for the Contributor or Provider Acceptance Levels.

7.3 Contributor

An Acceptance Level of Contributor correlates to a CNA's level of quality being considered equal to the NVD Initial Analyst output. Display on the NVD website follows the same requirements as the Reference Acceptance Level; however, there will be additional acknowledgement that the CNA is at a higher level of acceptance. As with Reference, only the NVD Analyst information will be available in the data feeds and web service content.

7.4 Provider

An Acceptance Level of Provider correlates to a CNA's level of quality considered equal to the NVD analyst during the Verification stage. Provider content will be the only content displayed within the CVE detail page on the NVD website with one exception: if the content is audited and determined to be incorrect by the NVD analyst, the NVD analyst content will be displayed on the NVD website, similar to the Reference and Contributor levels. If the audit determines that the

315 CNA content is correct, the Provider's content will be acknowledged as audited and approved by
316 the NVD.

8 CNA Acceptance Process

Participation in the submission process automatically begins when the CNA includes Submission Category information within their provided CVE entries. As submissions are received and NVD analysts complete Verification of CVEs, an email will be sent to the CNA to notify them that an audit has occurred and provide a link to the audit results. Once the CNA provides 40 CVE entries that contain information for a specific Submission Category(ies), a determination of Acceptance Level will be made.

The sample size of 40 has been selected based on the experience that it takes a new NVD analyst approximately 40 CVEs to become proficient in providing CVE metadata. While this requirement may be difficult to achieve for smaller CNAs in a timely manner, it is necessary to maintain the integrity of the NVD data. The NVD user base is comprised of thousands of businesses and local, state, and federal government agencies that rely on the NVD to provide a consistent result set. As this process matures, improvements and efficiencies may be achieved to allow for a reduction in the sample size. The Acceptance Thresholds defined below will be applied to determine what Acceptance Level the CNA's information will be assigned within the NVD.

9 Continuous Reporting and Auditing of CNAs

All participating CNAs will receive an email notice that an audit has occurred. The email will specify the results of the audit (success or failure) as well as provide a link to the NVD web page to view the audit report. The audit report will display the differences between the CNA and the NVD analyst results for the Submission Category, as well as a historical view of all previous audit reports. After reviewing the audit report, the CNAs may update the CVE JSON files to align with the NVD analyst results or provide additional publicly available data to assist in collaboration. These updates will be included within the next audit and will be used to determine the proper Acceptance Level assignment. The auditing rules are defined below for each Acceptance Level.

9.1 Contributor and Reference Acceptance Level Audit Schedule

For CNAs at the Acceptance Level of Reference or Contributor, there will be a continuous audit of the 40 most recent (new or modified) CVE entries. Audits will occur on a daily basis but only for CNAs who have submitted new or updated CVE entries or if the NVD analyst has made a change to a CNA's CVE entry.

9.2 Provider Acceptance Level Audit Schedule

For CNAs at the Provider Acceptance Level, the audit will consist of 40 recent CVE entries with one out of 10 CVE entries randomly selected for audit.

9.3 CNAs Exceeding Current Acceptance Level

At any given time, if the CNA is providing content for a Submission Category at the next Acceptance Level, they will automatically be moved to that Acceptance Level.

9.4 CNAs Not Meeting Acceptance Level

CNAs who do not meet their current Acceptance Level may become subject to an Acceptance Level reduction 30 days from their first failure. This gives the CNA ample opportunity to update their methodology to re-align with the NVD or to improve the available information so that the CNA analyst and NVD analyst can come to a consensus. Once a consensus is met, the CNA will meet or exceed their Acceptance Level.

10 Approval Thresholds and Calculations for Acceptance Level

10.1 CVSS v3.1 Base Metric Group

The CVSS v3.1 Base Metric Group consists of eight metrics. The CNA will be evaluated on 40 CVEs for a total of 320 metrics. The Acceptance Level match percentage will be calculated by taking the number of CNA CVE-to-CVSS metric combinations that match the NVD analyst metric combinations divided by the total number of NVD analyst metric combinations (320).

10.2 CVSS v2 Base Metric Group

The CVSS v2 Base Metric Group consists of six metrics. The CNA will be evaluated on 40 CVEs for a total of 240 metrics. The Acceptance Level match percentage will be calculated by taking the number of CNA CVE-to-CVSS metric combinations that match the NVD Analyst metric combinations divided by the total number of NVD Analyst metric combinations (240).

10.3 CWE

The CWE is a large list of values, and each CVE has the potential to have one or more of these values assigned. The Acceptance Level match percentage will be calculated by taking the number of CNA CVE-to-CWE combinations that match the NVD Analyst CVE-to-CWE combinations divided by the total number of NVD Analyst CVE-to-CWE metric combinations.

10.4 Reference Link Tag

The Reference Link Tag consists of a list of values. The Acceptance Level match percentage will be calculated by taking the CNA Reference Link Type-to-Reference to CVE combinations that match the NVD analyst Reference Link Type-to-Reference to CVE combinations divided by the total number of NVD analyst Reference Link Type-to-Reference to CVE combinations.

10.5 Configuration

Due to the complexity of Configurations, each CVE will be reviewed on a pass/fail evaluation. The NVD analyst will review the Configurations submitted and determine if the proper Configurations, CPE Match strings, and CPEs were applied and named consistently with NVD-defined processes. CNA Configurations will only be displayed or acknowledged when an Acceptance Level of Provider is achieved. The pass/fail evaluation will be determined by how closely it matches a Configuration and not that every expected Configuration has been provided. The Acceptance Level percentage will be calculated by taking the total number of passed Configurations and dividing it by the CVE audit size (40).

10.6 Acceptance Level Calculations

Table 3 identifies the explicit number ranges that must match the NVD analyst results in order to achieve a specific Acceptance Level.

393 **Table 3: Acceptance Level Match Range Per Submission Category (where possible)[6]**

Submission Category	Total	Reference	Contributor	Provider
CVSS v3.1 Base Metric Group	320	< 224 (< 70%)	>= 224 (>= 70%)	>= 304 (>= 95%)
CVSS v2 Base Metric Group	240	< 168 (< 70%)	>= 168 (>= 70%)	>= 228 (>= 95%)
CWE	--	< 70%	>= 70%	>= 95%
Reference Link Type	--	< 70%	>= 70%	>= 95%
Configuration	40	--	--	>=34

394

6 These values are accurate as of the publication date of this report. For the most current values, see table 1 in https://csrc.nist.gov/publications/detail/nistir/8246/draft.

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CNA	CVE Numbering Authority
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
FOIA	Freedom of Information Act
ID	Identifier
IR	Interagency or Internal Report
ITL	Information Technology Laboratory
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
SWID	Software Identification (Tag)
VDB	Vulnerability Database

Appendix B—Glossary

CVE Metadata	Information attached to the CVE by the NVD Analyst and/or CNA. Comprised of CVSS v3.1, CVSS v2, CWE, Reference Link Tags, and Configurations.
Initial Analysis	Internal phase within the NVD where an NVD Analyst begins to review a CVE and adds the appropriate metadata.
Verification	Internal phase within the NVD where a second, usually more experienced, NVD Analyst verifies the work completed during the Initial Analysis.

Appendix C—CVSS v3.1 Base Metric Group JSON Schema and Sample Data

JSON Schema:

```
"def_impact": {
            "type": "object",
            "properties": {
                "type": "object",
                "properties": {
                    "cvss": {"$ref": "cvss-v3.1.json"},
:
                    }
                },
            }
        },
```

JSON Sample:

```
"impact" : {
  "cvss" : {
    "version" : "3.1",
    "vectorString" : "CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
  },
```

Appendix D—CVSS v2 Base Metric Group JSON Schema and Sample Data

JSON Schema:

```
"def_impact": {
            "type": "object",
            "properties": {
                "type": "object",
                "properties": {
                    "cvss": {"$ref": "cvss-v2.0.json"},
:
                }
            }
        },
```

JSON Sample:

```
"impact" : {
      "cvss" : {
        "version" : "2.0",
        "vectorString" : "AV:N/AC:L/Au:S/C:P/I:P/A:P",
      },
    },
```

Appendix E—CWE JSON Schema and Sample Data

JSON Schema:

```
    "problemtype": {
      "type": "object",
      "required": [ "problemtype_data" ],
      "properties": {
        "problemtype_data": {
          "type": "array",
          "minItems": 0,
          "items": {
            "type": "object",
            "required": [ "description" ],
            "properties": {
              "description": {
                "type": "array",
                "minItems": 0,
                "items": { "$ref": "#/definitions/lang_string" }
              }
            }
          }
        }
      }
    },
```

JSON Sample:

```
"problemtype" : {
        "problemtype_data" : [ {
          "description" : [ {
            "lang" : "en",
            "value" : "CWE-264"
          } ]
        } ]
      },
```

Appendix F—Reference Tag JSON Schema and Sample Data

JSON Schema:

```
"references": {
      "type": "object",
      "required": [ "reference_data" ],
      "properties": {
        "reference_data": {
          "type": "array",
          "maxItems": 500,
          "minItems": 0,
          "items": { "$ref": "#/definitions/reference" }
        }
      }
    },
```

JSON Sample:

```
"references" : {
        "reference_data" : [ {
          "url" : "https://github.com/select2/select2/issues/4587",
          "name" : "https://github.com/select2/select2/issues/4587",
          "refsource" : "MISC",
          "tags" : [ "Third Party Advisory" ]
        }, {
          "url" : "https://github.com/snipe/snipe-it/pull/6831",
          "name" : "https://github.com/snipe/snipe-it/pull/6831",
          "refsource" : "MISC",
          "tags" : [ "Patch", "Third Party Advisory" ]
        } ]
      },
```

Appendix G—Configuration JSON Schema and Sample Data

JSON Schema:

```
"def_cve_item": {
            "description": "Defines a vulnerability in the NVD data feed.",
            "properties": {
                "cve": {"$ref": "CVE_JSON_4.0_min.schema"},
                "configurations": {"$ref":
"#/definitions/def_configurations"},
                "impact": {"$ref": "#/definitions/def_impact"},
                "publishedDate": {"type": "string"},
                "lastModifiedDate": {"type": "string"}
            },
            "required": ["cve"]
        }


   "def_configurations": {
            "description": "Defines the set of product configurations for a
NVD applicability statement.",
            "properties": {
                "CVE_data_version": {"type": "string"},
                "nodes": {
                    "type": "array",
                    "items": {"$ref": "#/definitions/def_node"}
                }
            },
            "required": [
                "CVE_data_version"
            ]
        },


   "def_node": {
            "description": "Defines a node or sub-node in an NVD
applicability statement.",
            "properties": {
                "operator": {"type": "string"},
                "negate": {"type": "boolean"},
                "children": {
                    "type": "array",
                    "items": {"$ref": "#/definitions/def_node"}
                },
                "cpe_match": {
                    "type": "array",
                    "items": {"$ref": "#/definitions/def_cpe_match"}
                }
            }
        },
```

```
    "def_cpe_match": {
        "description": "CPE match string or range",
        "type": "object",
        "properties": {
          "vulnerable": {
            "type": "boolean"
          },
          "cpe22Uri": {
            "type": "string"
          },
          "cpe23Uri": {
            "type": "string"
          },
          "versionStartExcluding": {
            "type": "string"
          },
          "versionStartIncluding": {
            "type": "string"
          },
          "versionEndExcluding": {
            "type": "string"
          },
          "versionEndIncluding": {
            "type": "string"
          },
          "cpe_name": {
            "type": "array",
            "items": {
              "$ref": "#/definitions/def_cpe_name"
            }
          }
        },
        "required": [
          "vulnerable",
          "cpe23Uri"
        ]
      },

  "def_cpe_name": {
        "description": "CPE name",
        "type": "object",
        "properties": {
          "cpe22Uri": {
            "type": "string"
          },
          "cpe23Uri": {
            "type": "string"
          }
        },
        "required": [
          "cpe23Uri"
        ]
      },
```

JSON Sample:

```
{
  "CVE_data_type" : "CVE",
  "CVE_data_format" : "MITRE",
  "CVE_data_version" : "4.0",
  "CVE_data_numberOfCVEs" : "2682",
  "CVE_data_timestamp" : "2019-04-24T07:00Z",
  "CVE_Items" : [ {
    "cve" : {
      "data_type" : "CVE",
      "data_format" : "MITRE",
      "data_version" : "4.0",
      "CVE_data_meta" : {
        "ID" : "CVE-2019-0001",
        "ASSIGNER" : "cve@mitre.org"
      },
  "configurations" : {
      "CVE_data_version" : "4.0",
      "nodes" : [ {
        "operator" : "OR",
        "cpe_match" : [ {
          "vulnerable" : true,
          "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:*:*:*:*:*:*:*"
          "cpe_name" : [ {
            "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:x:*:*:*:*:*:*"
            "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:y:*:*:*:*:*:*"
          } ]
        }, {
          "vulnerable" : true,
          "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:r1:*:*:*:*:*:*"
          "cpe_name" : [ {
            "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:r1:x:*:*:*:*:*"
            "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:r1:y:*:*:*:*:*"
        } ]
    },
```