NISTIR 8246

Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for 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

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

NISTIR 8246

Collaborative Vulnerability Metadata Acceptance Process (CVMAP) for CVE Numbering Authorities (CNAs) and Authorized Data Publishers

Robert Byers
David Waltermire
Chris Turner
Computer Security Division
Information Technology Laboratory

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

December 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
26 pages (December 2020)

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

Comments on this publication may be submitted to:

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 record metadata provided by the National Vulnerability Database (NVD) analysts through the formalization of a CVE record metadata submission process. This process will enable outside entities to submit CVE record metadata and allow this data to be presented to the end user with little to no NVD analyst involvement. For instances where the CVE record metadata is provided, the NVD analyst will serve in the role of auditor to ensure that consistent transparency and quality standards are applied, maintained, and communicated. Public recognition of the upstream participants' level of effort and consistency 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, CVE Authorized Data Publishers, and downstream consumers of NVD CVE data feeds.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

1 Introduction 1
2 Purpose and Scope 2
3 Roles and Responsibilities 3
4 Current NVD Analyst Workflow 4
5 External Submission Workflow 5
6 Submission Categories 6
6.1 CVSS v3.1 Base Metric Group 6
6.2 CVSS v2 Base Metric Group 6
6.3 CWE 6
6.4 Reference Link Tags 7
6.5 Configurations 7
7 Acceptance Levels 8
8 CNA Acceptance Process 9
9 Continuous Reporting and Auditing of CNAs 10
10 Approval Thresholds and Calculations for Acceptance Level 11
10.1 CVSS v3.1 Base Metric Group 11
10.2 CVSS v2 Base Metric Group 11
10.3 CWE 11
10.4 Reference Link Tag 11
10.5 Configuration 11

List of Appendices

Appendix A— Acronyms 12
Appendix B— Glossary 13
Appendix C— CVSS v3.1 Base Metric Group JSON Schema and Sample Data 14
Appendix D— CVSS v2 Base Metric Group JSON Schema and Sample Data 15
Appendix E— CWE JSON Schema and Sample Data 16
Appendix F— Reference Tag JSON Schema and Sample Data 17
Appendix G— Configuration JSON Schema and Sample Data 18

1 Introduction

The number of Common Vulnerabilities and Exposures (CVE) 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 limited resources. Decoupling efforts within the CVE program 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. The CVE program still maintains an oversight role for CNAs to ensure that proper procedures, content quality, and content consistency are maintained within the CVE program. By delegating the publication of CVE records 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 with reduced latency, improving the security of national IT infrastructure for both public and private entities.

As a result of the CVE program's success in delegating the CVE process to 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 in CVE records provided by these entities follow the same consistent criteria applied by the NVD analysts across all CVE records, 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 record metadata provided by the NVD analysts through the formalization of a CVE record metadata submission process. This process, referred to as Collaborative Vulnerability Metadata Acceptance Process (CVMAP), will enable outside entities to submit CVE record metadata and allow this data to be presented to the NVD end user with little to no NVD analyst involvement. For instances where the CVE record metadata is provided, the NVD analyst will serve in the role of auditor to ensure that transparency and consistency standards are applied, maintained, and communicated. Public recognition of the upstream participants' level of effort and consistency of data will be displayed on the CVE detail page within the public NVD website to encourage and incentivize participation. Although many CVE records received by the NVD will not provide this metadata, there are many entities participating in the CVE Program that have the interest and expertise to do so. The CNA has the following incentives to participate in CVMAP:

- The CNA can set the initial CVSS vector string.
- The CNA score/CWEs are shown on the NVD website regardless of whether they match the NVD analyst score/CWEs. This allows the CNA to communicate its findings to the user community.
- The CNA displays to peers and the user community that it is a mature CNA organization capable of providing defensible scores and metadata.
- Dialog is supported between the NVD analysts and the CNA analysts, which improves the consistency of metadata and drives improvement to scoring standards and advisory practices.

Although it is difficult to predict actual CVE growth and the participation levels of CNAs in the submission process, it is expected that once this process is in place and adopted, CNAs will be able to fully take advantage of their product expertise and provide accurate vulnerability metadata while also providing some relief to the continuously growing workload faced by the NVD.

3 Roles and Responsibilities

This section identifies the roles and responsibilities for entities that provide CVE record metadata.

Table 1: CVE Record Metadata Contribution Roles and Responsibilities

NVD Analyst	The NVD staff that provides the CVSS scores, CWEs, reference tags, and configuration information attached to the CVE within the NVD.
CVE Numbering Authority (CNA)	An organization responsible for the regular assignment of CVE IDs to vulnerabilities and for creating and publishing information about the vulnerability in the associated CVE record. Each CNA has a specific scope of responsibility for vulnerability identification and publishing.
Authorized Data Publisher (ADP)	An organization authorized within the CVE Program to enrich a CVE record previously published by a CNA with additional, related information, such as risk scores, affected product lists, and versions (i.e., references, translations) within a defined scope.

4 Current NVD Analyst Workflow

The current NVD analyst workflow for a single CVE record consists of two primary stages: 1) Initial Analysis and 2) Verification. Initial Analysis involves an NVD analyst investigating the information provided for the CVE record 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 v2 and CVSS v3.1 vector strings, associates CWE(s) with the CVE record, determines the appropriate Reference Link Tags, and builds the configurations using matching criteria defined in the Common Platform Enumeration (CPE) 2.3 specification.

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

5 External Submission Workflow

The External Submission process for both the CNA and the ADP begins by editing the CVE record JavaScript Object Notation (JSON) as noted in Appendices C, D, E, and F and following the approval process defined by the CVE program (https://cve.mitre.org/cve/cna.html). This process is the only mechanism in place for providing CVE record metadata. CNAs and ADPs 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 record 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 ADP is utilized by the NVD analyst as reference data and displayed on the public NVD website as well.

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 record JSON. There are no dependencies between the submission categories, and each submission category is optional. Both CNAs and ADPs 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 record. This categorization allows the end user to quickly identify relevant reference links. Valid Reference Link Tag Values are available at https://cwe.mitre.org.

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 record. 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

Please refer to https://nvd.nist.gov/vuln/cvmap/Understanding-Acceptance-Levels for up-to-date information on acceptance levels.

8 CNA Acceptance Process

Participation in the submission process automatically begins when the CNA includes submission category information within their provided CVE records. As submissions are received and NVD analysts complete a Verification of CVE records, 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 the acceptable number of CVE records that contain information for a specific submission category, a determination of acceptance level will be made.

A sample size has been selected based on the experience that it takes a new NVD analyst to become proficient in providing CVE record metadata. The current sample size can be found at https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels for each submission category provided. While this requirement may be difficult to achieve for smaller CNAs in a short period of time, it is necessary in order to maintain the consistency 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 (match or mismatch) and provide a public link to the NVD website 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 record 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 at https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels.

10 Approval Thresholds and Calculations for Acceptance Level

10.1 CVSS v3.1 Base Metric Group

Please refer to https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels#CVSSv31 for up-to-date information on CVSS v3.1 approval thresholds and acceptance level calculations.

10.2 CVSS v2 Base Metric Group

Please refer to https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels#CVSSv20 for up-to-date information on CVSS v2 approval thresholds and acceptance level calculations.

10.3 CWE

Please refer to https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels#CWE for up-to-date information on CWE approval thresholds and acceptance level calculations.

10.4 Reference Link Tag

Please refer to https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels#RefTag for up-to-date information on reference tag approval thresholds and acceptance level calculations.

10.5 Configuration

Please refer to https://nvd.nist.gov/vuln/cvmap/How-We-Assess-Acceptance-Levels#Config for up-to-date information on Configuration approval thresholds and acceptance level calculations.

Appendix A—Acronyms

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

ADP	Authorized Data Publisher
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
CVE ID	Common Vulnerabilities and Exposures identifiers
IR	Interagency or Internal Report
ITL	Information Technology Laboratory
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database

Appendix B—Glossary

CVE Record 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 (CVE record 4.0 format):

```
"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 (CVE record 4.0 format):

```
"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 (CVE record 4.0 format):

```
    "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 (CVE record 4.0 format):

```
"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 (CVE record 4.0 format):

```
"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:*:*:*:*:*"
        } ]
    },
```