

**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 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*

49 National Institute of Standards and Technology Interagency or Internal Report 8246  
50 30 pages (February 2020)

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

53 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an  
54 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or  
55 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best  
56 available for the purpose.

57 There may be references in this publication to other publications currently under development by NIST in accordance  
58 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,  
59 may be used by federal agencies even before the completion of such companion publications. Thus, until each  
60 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For  
61 planning and transition purposes, federal agencies may wish to closely follow the development of these new  
62 publications by NIST.

63 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to  
64 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at  
65 <https://csrc.nist.gov/publications>.

66

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

68 National Institute of Standards and Technology  
69 Attn: Computer Security Division, Information Technology Laboratory  
70 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930  
71 Email: [NISTIR\\_8246-Comments@nist.gov](mailto:NISTIR_8246-Comments@nist.gov)

72 All comments are subject to release under the Freedom of Information Act (FOIA).

73

74

## Reports on Computer Systems Technology

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

83

### Abstract

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

94

95

### Keywords

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

98

99

### Audience

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

102

103

104

**Call for Patent Claims**

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

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

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

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

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

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

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

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

129 Such statements should be addressed to: [NISTIR\\_8246-Comments@nist.gov](mailto:NISTIR_8246-Comments@nist.gov)

130 **Table of Contents**

131 **1 Introduction..... 1**

132 **2 Purpose and Scope..... 2**

133 **3 Roles and Responsibilities..... 3**

134 **4 Current NVD Analyst Workflow..... 4**

135 **5 External Submission Workflow..... 5**

136 **6 Submission Categories ..... 6**

137 6.1 CVSS v3.1 Base Metric Group..... 6

138 6.2 CVSS v2 Base Metric Group..... 6

139 6.3 CWE ..... 6

140 6.4 Reference Link Tags..... 7

141 6.5 Configurations..... 8

142 **7 Acceptance Levels..... 9**

143 7.1 Non-Acceptance ..... 9

144 7.2 Reference ..... 9

145 7.3 Contributor ..... 9

146 7.4 Provider ..... 9

147 **8 CNA Acceptance Process ..... 11**

148 **9 Continuous Reporting and Auditing of CNAs ..... 12**

149 9.1 Contributor and Reference Acceptance Level Audit Schedule ..... 12

150 9.2 Provider Acceptance Level Audit Schedule ..... 12

151 9.3 CNAs Exceeding Current Acceptance Level..... 12

152 9.4 CNAs Not Meeting Acceptance Level..... 12

153 **10 Approval Thresholds and Calculations for Acceptance Level..... 13**

154 10.1 CVSS v3.1 Base Metric Group..... 13

155 10.2 CVSS v2 Base Metric Group..... 13

156 10.3 CWE ..... 13

157 10.4 Reference Link Tag..... 13

158 10.5 Configuration..... 13

159 10.6 Acceptance Level Calculations ..... 13

160

161 **List of Appendices**

162 **Appendix A— Acronyms ..... 15**

163 **Appendix B— Glossary ..... 16**

164 **Appendix C— CVSS v3.1 Base Metric Group JSON Schema and Sample Data .... 17**

165 **Appendix D— CVSS v2 Base Metric Group JSON Schema and Sample Data ..... 18**

166 **Appendix E— CWE JSON Schema and Sample Data ..... 19**

167 **Appendix F— Reference Tag JSON Schema and Sample Data ..... 20**

168 **Appendix G— Configuration JSON Schema and Sample Data..... 21**

169

**1 Introduction**

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

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



**2 Purpose and Scope**

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

208

### 209 **3 Roles and Responsibilities**

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

211 **Table 1: CVE Entry Metadata Contribution Roles and Responsibilities**

<b>NVD Analyst</b>	The NVD staff responsible for the entry and oversight of the CVE entry metadata created by the NVD
<b>CVE Numbering Authority (CNA)</b>	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.
<b>Authorized Data Publisher</b>	The entity providing additional data related to a previously populated CVE entry within a distinct, agreed-upon scope

212

**213 4 Current NVD Analyst Workflow**

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

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

## 227 **5 External Submission Workflow**

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

238 Additional details are provided in the [Submission Categories](#) and [Acceptance Levels](#) sections  
239 later in this document.

## 240 **6 Submission Categories**

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

- 246 • CVSS v3.1 Base Metric Group
- 247 • CVSS v2 Base Metric Group
- 248 • CWEs
- 249 • Reference Link Tags
- 250 • Configurations

### 251 **6.1 CVSS v3.1 Base Metric Group**

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

### 257 **6.2 CVSS v2 Base Metric Group**

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

### 263 **6.3 CWE**

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

---

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

<sup>2</sup> 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>.

<sup>3</sup> 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>

<sup>4</sup> <https://cwe.mitre.org/>

268 **6.4 Reference Link Tags**

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

272 **Table 2: Valid Reference Link Tag Values**

Reference Link Tag Value	Description
<b>U.S. Government Resource</b>	The reference link is from a U.S. Government agency or organization (.mil or .gov).
<b>VDB Entry</b>	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: <a href="https://www.first.org/global/sigs/vrdx/vdb-catalog">https://www.first.org/global/sigs/vrdx/vdb-catalog</a>
<b>Vendor Advisory</b>	The advisory is from the vendor/publisher of the product or the parent company that owns the vendor.
<b>Third-Party Advisory</b>	The advisory is from an organization that is not the vulnerable product's vendor or publisher (or the vendor or publisher's parent company).
<b>Patch</b>	The reference contains an update to the software that fixes the vulnerability.
<b>Mitigation</b>	The reference contains information on steps to mitigate the vulnerability in the event a patch cannot be applied or is unavailable.
<b>Exploit</b>	The reference contains an in-depth, detailed description of steps to exploit a vulnerability or any legitimate POC code or exploit kit.
<b>Press/Media Coverage</b>	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.
<b>Issue Tracking</b>	The reference is a post from a bug tracking tool.
<b>Mailing List</b>	The reference is from a mailing list, often specific to a product or vendor.
<b>Release Notes</b>	The reference is in the format of a vendor or open-source project's release notes or change log.
<b>Technical Description</b>	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
<b>Product</b>	The reference is appropriate for describing a product for the purposes of a CPE ID or a Software Identification (SWID) Tag.
<b>Permissions Required</b>	The reference link provided is blocked by a login page. If credentials are required to see any information, this tag must be applied.

273 See Appendix F for accepted JSON schema and sample data.

## 274 **6.5 Configurations**

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

---

<sup>5</sup> <https://nvd.nist.gov/vuln/vulnerability-detail-pages>

## 280 **7 Acceptance Levels**

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

- 284 • Non-Acceptance
- 285 • Reference
- 286 • Contributor
- 287 • Provider

### 288 **7.1 Non-Acceptance**

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

### 292 **7.2 Reference**

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

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

### 303 **7.3 Contributor**

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

### 309 **7.4 Provider**

310 An Acceptance Level of Provider correlates to a CNA's level of quality considered equal to the  
311 NVD analyst during the Verification stage. Provider content will be the only content displayed  
312 within the CVE detail page on the NVD website with one exception: if the content is audited and  
313 determined to be incorrect by the NVD analyst, the NVD analyst content will be displayed on the  
314 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**

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

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

## 333 **9 Continuous Reporting and Auditing of CNAs**

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

### 343 **9.1 Contributor and Reference Acceptance Level Audit Schedule**

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

### 348 **9.2 Provider Acceptance Level Audit Schedule**

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

### 351 **9.3 CNAs Exceeding Current Acceptance Level**

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

### 354 **9.4 CNAs Not Meeting Acceptance Level**

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

## 360 **10 Approval Thresholds and Calculations for Acceptance Level**

### 361 **10.1 CVSS v3.1 Base Metric Group**

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

### 366 **10.2 CVSS v2 Base Metric Group**

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

### 371 **10.3 CWE**

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

### 376 **10.4 Reference Link Tag**

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

### 381 **10.5 Configuration**

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

### 390 **10.6 Acceptance Level Calculations**

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

393

**Table 3: Acceptance Level Match Range Per Submission Category (where possible)<sup>6</sup>**

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

394

---

<sup>6</sup> 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>.

**395 Appendix A—Acronyms**

396 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

397

398 **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.

399

400

**401 Appendix C—CVSS v3.1 Base Metric Group JSON Schema and Sample Data****402 JSON Schema:**

```
403 "def_impact": {  
404     "type": "object",  
405     "properties": {  
406         "type": "object",  
407         "properties": {  
408             "cvss": {"$ref": "cvss-v3.1.json"},  
409         }  
410     },  
411 },  
412 },  
413 },  
414
```

**415 JSON Sample:**

```
416 "impact" : {  
417     "cvss" : {  
418         "version" : "3.1",  
419         "vectorString" : "CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",  
420     },  
421 },  
422
```



**423 Appendix D—CVSS v2 Base Metric Group JSON Schema and Sample Data****424 JSON Schema:**

```
425 "def_impact": {
426     "type": "object",
427     "properties": {
428         "type": "object",
429         "properties": {
430             "cvss": {"$ref": "cvss-v2.0.json"},
431         }
432     }
433 },
```

**435 JSON Sample:**

```
436 "impact" : {
437     "cvss" : {
438         "version" : "2.0",
439         "vectorString" : "AV:N/AC:L/Au:S/C:P/I:P/A:P",
440     },
441 },
442
```

443 **Appendix E—CWE JSON Schema and Sample Data**444 **JSON Schema:**

```

445     "problemtype": {
446       "type": "object",
447       "required": [ "problemtype_data" ],
448       "properties": {
449         "problemtype_data": {
450           "type": "array",
451           "minItems": 0,
452           "items": {
453             "type": "object",
454             "required": [ "description" ],
455             "properties": {
456               "description": {
457                 "type": "array",
458                 "minItems": 0,
459                 "items": { "$ref": "#/definitions/lang_string" }
460               }
461             }
462           }
463         }
464       },
465     },
466

```

467 **JSON Sample:**

```

468 "problemtype" : {
469   "problemtype_data" : [ {
470     "description" : [ {
471       "lang" : "en",
472       "value" : "CWE-264"
473     } ]
474   } ]
475 },
476

```

**477 Appendix F—Reference Tag JSON Schema and Sample Data****478 JSON Schema:**

```
479 "references": {
480     "type": "object",
481     "required": [ "reference_data" ],
482     "properties": {
483         "reference_data": {
484             "type": "array",
485             "maxItems": 500,
486             "minItems": 0,
487             "items": { "$ref": "#/definitions/reference" }
488         }
489     }
490 },
491
```

**492 JSON Sample:**

```
493 "references" : {
494     "reference_data" : [ {
495         "url" : "https://github.com/select2/select2/issues/4587",
496         "name" : "https://github.com/select2/select2/issues/4587",
497         "refsource" : "MISC",
498         "tags" : [ "Third Party Advisory" ]
499     }, {
500         "url" : "https://github.com/snipe/snipe-it/pull/6831",
501         "name" : "https://github.com/snipe/snipe-it/pull/6831",
502         "refsource" : "MISC",
503         "tags" : [ "Patch", "Third Party Advisory" ]
504     } ]
505 },
506
```

507 **Appendix G—Configuration JSON Schema and Sample Data**508 **JSON Schema:**

```

509 "def_cve_item": {
510     "description": "Defines a vulnerability in the NVD data feed.",
511     "properties": {
512         "cve": {"$ref": "CVE_JSON_4.0_min.schema"},
513         "configurations": {"$ref":
514 "#/definitions/def_configurations"},
515         "impact": {"$ref": "#/definitions/def_impact"},
516         "publishedDate": {"type": "string"},
517         "lastModifiedDate": {"type": "string"}
518     },
519     "required": ["cve"]
520 }
521
522
523     "def_configurations": {
524         "description": "Defines the set of product configurations for a
525 NVD applicability statement.",
526         "properties": {
527             "CVE_data_version": {"type": "string"},
528             "nodes": {
529                 "type": "array",
530                 "items": {"$ref": "#/definitions/def_node"}
531             }
532         },
533         "required": [
534             "CVE_data_version"
535         ]
536     },
537
538
539     "def_node": {
540         "description": "Defines a node or sub-node in an NVD
541 applicability statement.",
542         "properties": {
543             "operator": {"type": "string"},
544             "negate": {"type": "boolean"},
545             "children": {
546                 "type": "array",
547                 "items": {"$ref": "#/definitions/def_node"}
548             },
549             "cpe_match": {
550                 "type": "array",
551                 "items": {"$ref": "#/definitions/def_cpe_match"}
552             }
553         }
554     },
555

```

```

556 "def_cpe_match": {
557   "description": "CPE match string or range",
558   "type": "object",
559   "properties": {
560     "vulnerable": {
561       "type": "boolean"
562     },
563     "cpe22Uri": {
564       "type": "string"
565     },
566     "cpe23Uri": {
567       "type": "string"
568     },
569     "versionStartExcluding": {
570       "type": "string"
571     },
572     "versionStartIncluding": {
573       "type": "string"
574     },
575     "versionEndExcluding": {
576       "type": "string"
577     },
578     "versionEndIncluding": {
579       "type": "string"
580     },
581     "cpe_name": {
582       "type": "array",
583       "items": {
584         "$ref": "#/definitions/def_cpe_name"
585       }
586     },
587   },
588   "required": [
589     "vulnerable",
590     "cpe23Uri"
591   ]
592 },
593
594 "def_cpe_name": {
595   "description": "CPE name",
596   "type": "object",
597   "properties": {
598     "cpe22Uri": {
599       "type": "string"
600     },
601     "cpe23Uri": {
602       "type": "string"
603     }
604   },
605   "required": [
606     "cpe23Uri"
607   ]
608 },

```

609

610 **JSON Sample:**

```

611 {
612   "CVE_data_type" : "CVE",
613   "CVE_data_format" : "MITRE",
614   "CVE_data_version" : "4.0",
615   "CVE_data_numberOfCVEs" : "2682",
616   "CVE_data_timestamp" : "2019-04-24T07:00Z",
617   "CVE_Items" : [ {
618     "cve" : {
619       "data_type" : "CVE",
620       "data_format" : "MITRE",
621       "data_version" : "4.0",
622       "CVE_data_meta" : {
623         "ID" : "CVE-2019-0001",
624         "ASSIGNER" : "cve@mitre.org"
625       },
626       "configurations" : {
627         "CVE_data_version" : "4.0",
628         "nodes" : [ {
629           "operator" : "OR",
630           "cpe_match" : [ {
631             "vulnerable" : true,
632             "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:*:*:*:*:*:*"
633             "cpe_name" : [ {
634               "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:x:*:*:*:*:*"
635               "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:y:*:*:*:*:*"
636             } ]
637           }, {
638             "vulnerable" : true,
639             "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:r1:*:*:*:*:*"
640             "cpe_name" : [ {
641               "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:r1:x:*:*:*:*:*"
642               "cpe23Uri" : "cpe:2.3:o:juniper:junos:16.1:r1:y:*:*:*:*:*"
643             } ]
644           },

```