Proposal for a CVSS v3.0 JSON Format, Version 1.0

# Introduction

CVSS v2.0 and v3.0 have defined formats for storing and transmitting CVSS information in XML format, specified as XML Schema Documents. There is growing interest in using JSON for the same purpose, so it makes sense to also define a JSON format. A introduction to the JSON format can be found at <http://www.json.org/>. A brief comparison between JSON and XML formats can be found at <https://www.w3schools.com/js/js_json_xml.asp>.

This document contains an informal description of a proposed JSON format for CVSS v3.0, some examples using this format, and an annex containing the formal JSON Schema definition.

# Informal Description of JSON Format

The JSON format is formally described in JSON schema format in Annex A - JSON Schema. If the informal explanation presented in this section conflicts with the JSON schema, the latter takes precedence.

CVSS v3.0 information is represented as a JSON object with the following fields:

* CVSS Version - mandatory and always **3.0**.
* Vector String - mandatory and specified with metrics in the *preferred order* described in the CVSS v3.0 Specification Document.
* Base Score - mandatory.
* Base Severity - mandatory.
* Individual metrics, i.e., Attack Vector, Attack Complexity, etc. - optional, but if included must match their respective values specified in the Vector String.
* Temporal Score - optional, but should be included if any Temporal Metrics are set to a non-default value.
* Temporal Severity - optional, but should be included if any Temporal Metrics are set to a non-default value.
* Environmental Score - optional, but should be included if any Environmental Metrics are set to a non-default value.
* Environmental Severity - optional, but should be included if any Environmental Metrics are set to a non-default value.

# References

|  |  |
| --- | --- |
| http://json.org/ | JSON Specification. |
| http://json-schema.org/ | JSON Schema Specification. |
| https://google.github.io/styleguide/jsoncstyleguide.xml | JSON Style Guide - from Google, but similar to other style guides. |
| https://jsonschemalint.com/#/version/draft-04/markup/json | A useful website for checking that JSON schemas and documents are well-formed, and validating a given JSON document against a given JSON schema. |
| https://www.first.org/cvss/cvss-v3.0.xsd?20150804 | CVSS v3.0 XML Schema Definition. |

# Example 1: Minimal Information Supplied

*Based on CVE-2009-0658 (Adobe Acrobat Buffer Overflow Vulnerability) from the CVSS v3.0 Examples Document.*

{

"version": "3.0",

"vectorString": "CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H",

"baseScore": 7.8,

"baseSeverity": "HIGH"

}

# Example 2: Optional Base Metrics Supplied

1. *Based on CVE-2009-0658 (Adobe Acrobat Buffer Overflow Vulnerability) from the CVSS v3.0 Examples Document.*
2. {
3. "version": "3.0",
4. "vectorString": "CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H",
5. "attackVector": "LOCAL",
6. "attackComplexity": "LOW",
7. "privilegesRequired": "NONE",
8. "userInteraction": "REQUIRED",
9. "scope": "UNCHANGED",
10. "confidentialityImpact": "HIGH",
11. "integrityImpact": "HIGH",
12. "availabilityImpact": "HIGH",
13. "baseScore": 7.8,
14. "baseSeverity": "HIGH"
15. }

# Example 3: Temporal and Environmental Metrics Included in Vector String

1. *Based on the Course Project in the CVSS v3.0 On-Line Course.*
2. {
3. "version": "3.0",
4. "vectorString": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H/E:P/RL:W/RC:U/CR:M/MI:N",
5. "baseScore": 10.0,
6. "baseSeverity": "CRITICAL",
7. "temporalScore": 8.4,
8. "temporalSeverity": "HIGH",
9. "environmentalScore": 7.3,
10. "environmentalSeverity": "HIGH"
11. }

# Example 4: Individual Temporal and Environmental Metrics Supplied

*Based on the Course Project in the CVSS v3.0 On-Line Course.*

{

"version": "3.0",

"vectorString": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H/E:P/RL:W/RC:U/CR:M/MI:N",

"attackVector": "NETWORK",

"attackComplexity": "LOW",

"privilegesRequired": "NONE",

"userInteraction": "NONE",

"scope": "CHANGED",

"confidentialityImpact": "NONE",

"integrityImpact": "HIGH",

"availabilityImpact": "HIGH",

"baseScore": 10.0,

"baseSeverity": "CRITICAL",

"exploitCodeMaturity": "PROOF\_OF\_CONCEPT",

"remediationLevel": "WORKAROUND",

"reportConfidence": "UNKNOWN",

"temporalScore": 8.4,

"temporalSeverity": "HIGH",

"confidentialityRequirement": "MEDIUM",

"modifiedIntegrityImpact": "NONE",

"environmentalScore": 7.3,

"environmentalSeverity": "HIGH"

}

# Annex A - JSON Schema

{

"$schema": "http://json-schema.org/draft-04/schema#",

"title": "JSON Schema for Common Vulnerability Scoring System version 3.0",

"id": "https://www.first.org/cvss/cvss-v3.0.json?20170424",

"type": "object",

"definitions": {

"attackVectorType": {

"type": "string",

"enum": [ "NETWORK", "ADJACENT\_NETWORK", "LOCAL", "PHYSICAL" ]

},

"modifiedAttackVectorType": {

"type": "string",

"enum": [ "NETWORK", "ADJACENT\_NETWORK", "LOCAL", "PHYSICAL", "NOT\_DEFINED" ]

},

"attackComplexityType": {

"type": "string",

"enum": [ "HIGH", "LOW" ]

},

"modifiedAttackComplexityType": {

"type": "string",

"enum": [ "HIGH", "LOW", "NOT\_DEFINED" ]

},

"privilegesRequiredType": {

"type": "string",

"enum": [ "HIGH", "LOW", "NONE" ]

},

"modifiedPrivilegesRequiredType": {

"type": "string",

"enum": [ "HIGH", "LOW", "NONE", "NOT\_DEFINED" ]

},

"userInteractionType": {

"type": "string",

"enum": [ "NONE", "REQUIRED" ]

},

"modifiedUserInteractionType": {

"type": "string",

"enum": [ "NONE", "REQUIRED", "NOT\_DEFINED" ]

},

"scopeType": {

"type": "string",

"enum": [ "UNCHANGED", "CHANGED" ]

},

"modifiedScopeType": {

"type": "string",

"enum": [ "UNCHANGED", "CHANGED", "NOT\_DEFINED" ]

},

"ciaType": {

"type": "string",

"enum": [ "NONE", "LOW", "HIGH" ]

},

"modifiedCiaType": {

"type": "string",

"enum": [ "NONE", "LOW", "HIGH", "NOT\_DEFINED" ]

},

"exploitCodeMaturityType": {

"type": "string",

"enum": [ "UNPROVEN", "PROOF\_OF\_CONCEPT", "FUNCTIONAL", "HIGH", "NOT\_DEFINED" ]

},

"remediationLevelType": {

"type": "string",

"enum": [ "OFFICIAL\_FIX", "TEMPORARY\_FIX", "WORKAROUND", "UNAVAILABLE", "NOT\_DEFINED" ]

},

"confidenceType": {

"type": "string",

"enum": [ "UNKNOWN", "REASONABLE", "CONFIRMED", "NOT\_DEFINED" ]

},

"ciaRequirementType": {

"type": "string",

"enum": [ "LOW", "MEDIUM", "HIGH", "NOT\_DEFINED" ]

},

"scoreType": {

"type": "number",

"minimum": 0,

"maximum": 10

},

"severityType": {

"type": "string",

"enum": [ "NONE", "LOW", "MEDIUM", "HIGH", "CRITICAL" ]

}

},

"properties": {

"version": {

"description": "CVSS Version",

"type": "string",

"enum": [ "3.0" ]

},

"vectorString": {

"type": "string",

"pattern": "^CVSS:3.0/((AV:[NALP]|AC:[LH]|PR:[UNLH]|UI:[NR]|S:[UC]|[CIA]:[NLH]|E:[XUPFH]|RL:[XOTWU]|RC:[XURC]|[CIA]R:[XLMH]|MAV:[XNALP]|MAC:[XLH]|MPR:[XUNLH]|MUI:[XNR]|MS:[XUC]|M[CIA]:[XNLH])/)\*(AV:[NALP]|AC:[LH]|PR:[UNLH]|UI:[NR]|S:[UC]|[CIA]:[NLH]|E:[XUPFH]|RL:[XOTWU]|RC:[XURC]|[CIA]R:[XLMH]|MAV:[XNALP]|MAC:[XLH]|MPR:[XUNLH]|MUI:[XNR]|MS:[XUC]|M[CIA]:[XNLH])$"

},

"attackVector": { "$ref": "#/definitions/attackVectorType" },

"attackComplexity": { "$ref": "#/definitions/attackComplexityType" },

"privilegesRequired": { "$ref": "#/definitions/privilegesRequiredType" },

"userInteraction": { "$ref": "#/definitions/userInteractionType" },

"scope": { "$ref": "#/definitions/scopeType" },

"confidentialityImpact": { "$ref": "#/definitions/ciaType" },

"integrityImpact": { "$ref": "#/definitions/ciaType" },

"availabilityImpact": { "$ref": "#/definitions/ciaType" },

"baseScore": { "$ref": "#/definitions/scoreType" },

"baseSeverity": { "$ref": "#/definitions/severityType" },

"exploitCodeMaturity": { "$ref": "#/definitions/exploitCodeMaturityType" },

"remediationLevel": { "$ref": "#/definitions/remediationLevelType" },

"reportConfidence": { "$ref": "#/definitions/confidenceType" },

"temporalScore": { "$ref": "#/definitions/scoreType" },

"temporalSeverity": { "$ref": "#/definitions/severityType" },

"confidentialityRequirement": { "$ref": "#/definitions/ciaRequirementType" },

"integrityRequirement": { "$ref": "#/definitions/ciaRequirementType" },

"availabilityRequirement": { "$ref": "#/definitions/ciaRequirementType" },

"modifiedAttackVector": { "$ref": "#/definitions/modifiedAttackVectorType" },

"modifiedAttackComplexity": { "$ref": "#/definitions/modifiedAttackComplexityType" },

"modifiedPrivilegesRequired": { "$ref": "#/definitions/modifiedPrivilegesRequiredType" },

"modifiedUserInteraction": { "$ref": "#/definitions/modifiedUserInteractionType" },

"modifiedScope": { "$ref": "#/definitions/modifiedScopeType" },

"modifiedConfidentialityImpact": { "$ref": "#/definitions/modifiedCiaType" },

"modifiedIntegrityImpact": { "$ref": "#/definitions/modifiedCiaType" },

"modifiedAvailabilityImpact": { "$ref": "#/definitions/modifiedCiaType" },

"environmentalScore": { "$ref": "#/definitions/scoreType" },

"environmentalSeverity": { "$ref": "#/definitions/severityType" }

},

"required": [ "version", "vectorString", "baseScore", "baseSeverity" ]

}