Static Analysis Results Interchange Format (SARIF) Version 2.1.0 Errata 01

OASIS Approved Errata

28 August 2023

This stage:
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/sarif-v2.1.0-errata01-os.docx (Authoritative)
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/sarif-v2.1.0-errata01-os.html
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/sarif-v2.1.0-errata01-os.pdf

Previous stage:
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/csd01/sarif-v2.1.0-errata01-csd01.docx (Authoritative)
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/csd01/sarif-v2.1.0-errata01-csd01.html
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/csd01/sarif-v2.1.0-errata01-csd01.pdf

Latest stage:
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/sarif-v2.1.0-errata01.docx (Authoritative)
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/sarif-v2.1.0-errata01.html
https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/sarif-v2.1.0-errata01.pdf

Technical Committee:
OASIS Static Analysis Results Interchange Format (SARIF) TC

Chairs:
David Keaton (dmk@dmk.com), Individual Member
Luke Cartey (lcartey@github.com), Microsoft

Editor:
Michael C. Fanning (mikefan@microsoft.com), Microsoft

Additional artifacts:
This document is one component of a Work Product that also includes:

- OASIS Standard with embedded Errata. *Static Analysis Results Interchange Format (SARIF) Version 2.1.0 Plus Errata01*. Edited by Michael C. Fanning and Laurence J. Golding. 28 August 2023. OASIS Standard incorporating Approved Errata 01. https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/sarif-v2.1.0-errata01-os-complete.html.
- Change-marked (redlined) OASIS Standard document. *Static Analysis Results Interchange Format (SARIF) Version 2.1.0 Plus Errata01 (redlined)*. Edited by Michael C. Fanning and Laurence J. Golding. 28 August 2023. OASIS Standard incorporating Approved Errata 01. https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/sarif-v2.1.0-errata01-os-redlined.html.
- The SARIF schema: https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/schemas/sarif-schema-2.1.0.json.
- The SARIF External Property File schema: https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/schemas/sarif-external-property-file-schema-2.1.0.json.

Related work:
This document lists Errata for:

- *Static Analysis Results Interchange Format (SARIF) Version 2.1.0*. Edited by Michael C. Fanning and Laurence J. Golding. 27 March 2020. OASIS Standard. https://docs.oasis-open.org/sarif/sarif/v2.1.0/os/sarif-v2.1.0-os.html.

Abstract:
This document lists Errata for the OASIS Standard *Static Analysis Results Interchange Format (SARIF) Version 2.1.0*.

Status:
This document was last revised or approved by the OASIS Static Analysis Results Interchange Format (SARIF) TC on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=sarif#technical.

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/sarif/.

This document is provided under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this document, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/sarif/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:
When referencing this document, the following citation format should be used:

[SARIF-v2.1.0-Errata01]

Static Analysis Results Interchange Format (SARIF) Version 2.1.0 Errata 01. Edited by Michael C. Fanning. 28 August 2023. OASIS Approved Errata. https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/os/sarif-v2.1.0-errata01-os.html. Latest stage: https://docs.oasis-open.org/sarif/sarif/v2.1.0/errata01/sarif-v2.1.0-errata01.html.

Notices:

Table of Contents

1 Introduction

This document lists the approved changes to Static Analysis Results Interchange Format (SARIF) Version 2.1.0 [SARIF].

Additional documents containing the final specification with these changes marked and included are also available and linked in the section "Additional artifacts" on the title page.

2 Changes to SARIF

Each of the changes to be included in SARIF upon approval of these Errata is listed in the following sections. The title of each section includes a link to the github issue along with explanatory text and material. The github repository with all issues is accessible at https://github.com/oasis-tcs/sarif-spec/issues/.

2.1 Issue #457: Bug in sample: "src/" => "bin/"

In the EXAMPLE in §3.4.6, change the `uri` for `BINROOT` from `".../src/"` to `".../bin/"`:

```
    "BINROOT": {
      "uri": "file:///C:/browser/bin/",
      "description": {
        "text": "The build output directory."
      }
    }
```

2.2 Issue #458: Some originalUriBaseIds uri properties in examples lack trailing slash

Add a trailing slash to 'originalUriBaseId' properties.

§3.14.14, EXAMPLE 1, `SRCROOT`:

```
"originalUriBaseIds": {
 "PROJECTROOT": {
    "uri": "file:///C:/Users/Mary/code/TheProject/",
    "description": {
      "text": "The root directory for all project files."
    }
 },
  "SRCROOT": {
    "uri": "src/",
    "uriBaseId": "PROJECTROOT",
    "description": {
      "text": "The root of the source tree."
    }
  }
}
```

```
"originalUriBaseIds": {
 "PROJECTROOT": {
    "description": {
      "text": "The root directory for all project files."
    }
 },
  "SRCROOT": {
    "uri": "src/",
    "uriBaseId": "PROJECTROOT",
    "description": {
      "text": "The root of the source tree."
    }
  }
}
```

§3.23.8, EXAMPLE, `HOME` and `PACKAGE_ROOT`:

```
"originalUriBaseIds": {
  "HOME": {
    "uri": "file:///home/user/"
  }
  "PACKAGE_ROOT": {
    "uri": "package/",
    "uriBaseId": "HOME"
  },
},
```

§3.25.2, EXAMPLE, `WEBHOST`:

```
"originalUriBaseIds": {   # See §3.14.14.
  "WEBHOST": {
    "uri": "http://www.example.com/"
  },
```

2.3 Issue #460: Explain why ".." path segments can't be normalized out

In §3.10.2, clarify that ".." segments can't be normalized in all cases due to the possibility of a reparse point.

> *NOTE 2: ".." path segments are dangerous because the semantics of the file system on which the SARIF log file was produced might not match the semantics of the file system on which it is consumed. For example, the presence of a symbolic link in the path might redirect the consumer to an unpredictable location.*

2.4 Issue #461: Discourage ".." in file scheme URIs

In §3.10.2, add the statement that consumers **SHOULD** reject paths that contain ".." segments.

SARIF consumers SHALL NOT normalize ".." segments out of a path. A consumer SHOULD reject paths that contain ".." segments, otherwise a consumer SHALL treat distinct portions of paths up to and including the rightmost ".." segment as unique directories on the file system, even if [RFC3986] normalization would produce identical paths.

2.5 Issue #462: Clarify that a region requires a "start" property.

In §3.30.1, clarify that a 'region' SHALL contain one of 'startLine', 'charOffset' or 'byteOffset'. Update SARIF schema with this constraint as well, by adding the following statement:

> *A region SHALL contain at least one of startLine, charOffset, or byteOffset.*

2.6 Issue #464: Clarify meaning of 'resultFile' artifact role.

In §3.24.6, clarify that 'resultFile' is only for files which haven't been explicitly configured as scan targets (in which case the 'analysisFile' role should be used).

- *"resultFile": A result was detected in this artifact (which the analysis tool was not explicitly instructed to scan).*

  NOTE 3: For example, a scanner might be configured to analyze a C source file and find a result in a header file that it includes. The header file may be marked with the "resultFile" role. The C file should be marked with the "analysisTarget" role, however, as it was explicitly configured as a scan target.

2.7 Issue #468: Recommend the path-noscheme form for relative URIs.

In §3.4.3, clarify that relative reference shall not take the form of a non-scheme absolute path reference (i.e., a single leading slash) except in cases when doing so distinguishes two distinct resources.

If a URI is a relative reference, it **SHALL NOT** begin with two slash characters (a 'network-path' reference per section 4.2 of [RFC3986]. A relative reference **SHALL NOT** begin with a single slash character (an 'absolute-path' reference per section 4.2 of [RFC3986]) unless doing so is required to distinguish between distinct items in archive formats, such as zip and tar.

Immediately before the NOTE that begins 'uri does not have to begin with a "/"', add:

> *NOTE 1: A relative path is useful to reference any artifact with a fixed location relative to a non-deterministic root, e.g., the relative version control path of a file as distinct from a local enlistment root. The uriBaseId (3.4.4) property can be used to express the non-deterministic absolute URI root. This approach assists in log file diffing and other scenarios where a clear distinction between data that is consistent or not between scan environments is helpful.*

2.8 Issue #476: Comprehensive SARIF file example is not a valid JSON.

In section K.4, update comprehensive SARIF file to make it valid content.

2.9 Issue #477: Add appendices for media type and URI scheme registrations.

Add normative reference to 1.3 for MIME registration process:

[RFC2048] N. Freed, J. Klensin, J. Postel, Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures, http://www.ietf.org/rfc/rfc2048.txt, IETF, 1996.

Add Appendix M. (Non-Normative) MIME Types and File Name Extensions:

The following is a list of MIME types and file extensions for files that conform to this specification, registered according to [RFC2048].

MIME type	*Extension*	*Description*
application/sarif+json	*.sarif,* *.sarif.json*	*SARIF log files (§3).*
application/sarif-external-properties+json	*.sarif-external-properties,* *.sarif-external-properties.json*	*SARIF external property files (§4).*

2.10 Issue #480: Don't allow leading / in relative artifact location URIs.

3.4.3. 'uri' property of 'artifactLocation'. Make it explicit that leading forward slashes are not permitted in artifact location URIs.

2.11 Issue #481: Schema doesn't allow sarifLog.runs to be null.

Schema should allow 'sarifLog.runs' to be a null value (indicating a catastrophic error was encountered during log file generation).

```
"runs": {
  "description": "The set of runs contained in this log file.",
  "type": [ "array", "null" ],
  "minItems": 0,
  "uniqueItems": false,
  "items": {
    "$ref": "#/definitions/run"
  }
```

2.12 Issue #487: Enums in the JSON Schema should include a type.

Provide explicit JSON type (which is universally “string”) for all schema enums.

```
"version": {
  "description": "The SARIF format version of this log file.",
  "enum": [ "2.1.0" ],
  "type": "string"
}
```

2.13 Issue #488: The schema of the `run.language` and `toolComponent.language` properties is incorrect.

Correct the regex pattern that validates ‘run.language’ and ‘toolComponent.language’ properties, to the following:

```
^[a-zA-Z]{2}(-[a-zA-Z]{2})?$
```

2.14 Issue #494: Update known misspellings across schema, spec, etc.

Correct misspellings of ‘identifer’ in SARIF schemas and ‘extermalized’ in the specification.

2.15 Issue #568: Miscellaneous final cleanup

- In the definition of ‘opaque‘ change ‘reable‘ to ‘readable‘.
- Change Luke Cartey’s company from Semmle to Microsoft.
- Put `version` before `$schema` in the examples to match the document’s suggestion.
- Enumerate both schemas explicitly under the artifacts section.
- Change all references to the schema URLs to point to the official OASIS location instead of github.
- Correct `"artifact"` in example K.3 to `"artifacts"`.
- Add the missing normative reference to ECMA-404.
- Fix the broken link to the definition of the term *artifact* in the definition of the term *result management system*.

3 Conformance

The Errata listed in this document do not modify the conformance requirements of SARIF.

Appendix A. References

This appendix contains the normative and informative references that are used in this document.

While any hyperlinks included in this appendix were valid at the time of publication, OASIS cannot guarantee their long-term validity.

A.1 Normative References

The following documents are referenced in such a way that some or all of their content constitutes requirements of this document.

[SARIF]

Static Analysis Results Interchange Format (SARIF) Version 2.1.0. Edited by Michael C. Fanning and Laurence J. Golding. 27 March 2020. OASIS Standard. https://docs.oasis-open.org/sarif/sarif/v2.1.0/os/sarif-v2.1.0-os.html.

Appendix B. Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website: [https://www.oasis-open.org/policies-guidelines/ipr/].

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OASIS AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this deliverable.]

[OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this OASIS Standards Final Deliverable. OASIS may include such claims on its website, but disclaims any obligation to do so.]

[OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this OASIS Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Standards Final Deliverable, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.]

The name "OASIS" is a trademark of OASIS, the owner and developer of this document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark/ for above guidance.