International Standard

ISO/IEC 20153

Information technology — OASIS Common Security Advisory Framework (CSAF) v2.0 Specification

First edition
2025-02

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-2025

Reference number
ISO/IEC 20153:2025(en)

© ISO/IEC 2025

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-2025

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025
All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940e-8dd5579a128b/iso-iec-20153-2025

This document was prepared by OASIS [as OASIS Common Security Advisory Framework (CSAF) TC] and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2025 – All rights reserved

Table of Contents

iTeh Standards
(https://standards.iteh.ai)
Document Preview
https://standards.iteh.ai/c...579a128b/iso-iec-20153-202

© ISO/IEC 2025 – All rights reserved

iTeh Standards (https://standards.iteh.ai) Document Preview ISO/IEC 20153:2025

© ISO/IEC 2025 – All rights reserved

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-202

© ISO/IEC 2025 – All rights reserved

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-202

© ISO/IEC 2025 – All rights reserved

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-202

© ISO/IEC 2025 – All rights reserved

1 Introduction

1.1 IPR Policy

This specification is provided under the Non-Assertion 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 specification, 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/csaf/ipr.php).

1.2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

For purposes of this document, the following terms and definitions apply:

advisory: reporting item that describes a condition present in an artifact and that requires action by the consumers

advisory document: artifact in which an analysis tool reports a result

advisory management system: software system that consumes the documents produced by analysis tools, produces advisories that enable engineering and operating organizations to assess the quality of these software artifacts at a point in time, and performs functions such as filing security advisories and displaying information about individual advisories. **Note**: An advisory management system can interact with a document viewer to display information about individual advisories.

advisory matching: process of determining whether two advisories are targeting the same products and conditions

artifact: sequence of bytes addressable via a URI. *Examples*: A physical file in a file system such as a source file, an object file, a configuration file or a data file; a specific version of a file in a version control system; a database table accessed via an HTTP request; an arbitrary stream of bytes returned from an HTTP request, a product URL, a common product enumeration value.

CSAF asset matching system: program that connects to or is an asset database and is able to manage CSAF documents as required by CSAF management system as well as matching them to assets of the asset database.

CSAF basic validator: A program that reads a document and checks it against the JSON schema and performs mandatory tests.

CSAF consumer: program that reads and interprets a CSAF document

CSAF content management system: program that is able to create, review and manage CSAF documents and is able to preview their details as required by CSAF viewer.

iTeh Standards (https://standards.iteh.ai) Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-2025

CSAF converter: CSAF producer that transforms the output of an analysis tool from its native output format into the CSAF format

CSAF direct producer: analysis tool which acts as a CSAF producer

CSAF document: security advisory text document in the format defined by this document.

CSAF extended validator: A CSAF basic validator that additionally performs optional tests.

CSAF full validator: A CSAF extended validator that additionally performs informative tests.

CSAF management system: program that is able to manage CSAF documents and is able to display their details as required by CSAF viewer.

CSAF modifier: CSAF post-processor which takes a CSAF document as input and modifies the structure or values of properties. The output is a valid CSAF document.

CSAF post-processor: CSAF producer that transforms an existing CSAF document into a new CSAF document, for example, by removing or redacting elements according to sharing policies.

CSAF SBOM matching system: A program that connects to or is an SBOM database and is able to manage CSAF documents as required by CSAF management system as well as matching them to SBOM components of the SBOM database.

CSAF producer: program that emits output in the CSAF format

CSAF translator: CSAF post-processor which takes a CSAF document as input and translates values of properties into another language. The output is a valid CSAF document.

CSAF viewer: CSAF consumer that reads a CSAF document, displays a list of the results it contains, and allows an end user to view each

© ISO/IEC 2025 – All rights reserved

result in the context of the artifact in which it occurs.

CVRF CSAF converter: CSAF producer which takes a CVRF document as input and converts it into a valid CSAF document.

document: output file produced by an analysis tool, which enumerates the results produced by the tool

driver: tool component containing an analysis tool's or converter's primary executable, which controls the tool's or converter's execution, and which in the case of an analysis tool typically defines a set of analysis rules

embedded link: syntactic construct which enables a message string to refer to a location mentioned in the document

empty array: array that contains no elements, and so has a length of 0

empty object: object that contains no properties

empty string: string that contains no characters, and so has a length of 0

(end) user: person who uses the information in a document to investigate, triage, or resolve results

engineering system: software analysis environment within which analysis tools execute. **Note**: An engineering system might include a build system, a source control system, a result management system, a bug tracking system, a test execution system, and so on.

extension: tool component other than the driver (for example, a plugin, a configuration file, or a taxonomy)

external property file: file containing the values of one or more externalized properties

externalizable property: property that can be contained in an external property file

externalized property: property stored outside of the CSAF document to which it logically belongs

false positive: result which an end user decides does not actually represent a problem

fingerprint: stable value that can be used by a result management system to uniquely identify a result over time, even if a relevant artifact is modified

formatted message: message string which contains formatting information such as Markdown formatting characters

fully qualified logical name: string that fully identifies the programmatic construct specified by a logical location, typically by means of a hierarchical identifier.

hierarchical string: string in the format <component>{/<component>}*

line: contiguous sequence of characters, starting either at the beginning of an artifact or immediately after a newline sequence, and ending at and including the nearest subsequent newline sequence, if one is present, or else extending to the end of the artifact

line (number): 1-based index of a line within a file. **Note**: Abbreviated to "line" when there is no danger of ambiguity with "line" in the sense of a sequence of characters.

localizable: subject to being translated from one natural language to another

message string: human-readable string that conveys information relevant to an element in a CSAF document

nested artifact: artifact that is contained within another artifact

newline sequence: sequence of one or more characters representing the end of a line of text. **Note**: Some systems represent a newline sequence with a single newline character; others represent it as a carriage return character followed by a newline character.

notification: reporting item that describes a condition encountered by a tool during its execution

opaque: neither human-readable nor machine-parsable into constituent parts

parent (artifact): artifact which contains one or more nested artifacts

plain text message: message string which does not contain any formatting information

plugin: tool component that defines additional rules

policy: set of rule configurations that specify how results that violate the rules defined by a particular tool component are to be treated

problem: result which indicates a condition that has the potential to detract from the quality of the program. *Examples*: A security vulnerability, a deviation from contractual or legal requirements.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/sist/...28b/iso-iec-20153-2025

© ISO/IEC 2025 – All rights reserved

product: is any deliverable (e.g. software, hardware, specification,...) which can be referred to with a name. This applies regardless of the origin, the license model, or the mode of distribution of the deliverable.

property: attribute of an object consisting of a name and a value associated with the name

redactable property: property that potentially contains sensitive information that a CSAF direct producer or a CSAF post-processor might wish to redact

reporting item: unit of output produced by a tool, either a result or a notification

reporting configuration: the subset of reporting metadata that a tool can configure at runtime, before performing its scan. *Examples*: severity level, rank

repository container for a related set of files in a version control system

taxonomy: classification of analysis results into a set of categories

tag: string that conveys additional information about the CSAF document element to which it applies

text artifact: artifact considered as a sequence of characters organized into lines and columns

text region: region representing a contiguous range of zero or more characters in a text artifact

tool component: component of an analysis tool or converter, either its driver or an extension, consisting of one or more files

top-level artifact: artifact which is not contained within any other artifact

translation: rendering of a tool component's localizable strings into another language

triage: decide whether a result indicates a problem that needs to be corrected

iTeh Standards

user: see end user.

VCS: version control system

(https://standards.iteh.ai)

vendor: the community, individual, or organization that created or maintains a product (including open source software and hardware providers)

Document Preview

VEX: Vulnerability Exploitability eXchange - enables a supplier or other party to assert whether or not a particular product is affected by a specific vulnerability, especially helpful in efficiently consuming SBOM data.

viewer: see CSAF viewer.

ISO/IEC 20153:2025

vulnerability: functional behavior of a product or service that violates an implicit or explicit security policy (conforming to ISO/IEC 29147 [ISO29147])

XML: eXtensible Markup Language - the format used by the predecessors of this standard, namely CVRF 1.1 and CVRF 1.2.

1.3 Normative References

[JSON-Schema-Core]

JSON Schema: A Media Type for Describing JSON Documents, draft-bhutton-json-schema-00, December 2020, https://datatracker.ietf.org/doc/html/draft-bhutton-json-schema-00.

[JSON-Schema-Validation]

JSON Schema Validation: A Vocabulary for Structural Validation of JSON, draft-bhutton-json-schema-validation-00, December 2020, https://datatracker.ietf.org/doc/html/draft-bhutton-json-schema-validation-00.

[JSON-Hyper-Schema]

JSON Hyper-Schema: A Vocabulary for Hypermedia Annotation of JSON, draft-handrews-json-schema-hyperschema-02, September 2019, https://json-schema.org/draft/2019-09/json-schema-hypermedia.html.

[Relative-JSON-Pointers]

Relative JSON Pointers, draft-bhutton-relative-json-pointer-00, December 2020, https://datatracker.ietf.org/doc/html/draft-bhutton-relative-json-pointer-00.

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997,

© ISO/IEC 2025 – All rights reserved

https://www.rfc-editor.org/info/rfc2119.

[RFC7464]

Williams, N., "JavaScript Object Notation (JSON) Text Sequences", RFC 7464, DOI 10.17487/RFC7464, February 2015, https://www.rfc-editor.org/info/rfc7464.

[RFC8174]

Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, https://www.rfc-editor.org/info/rfc8174.

[RFC8259]

T. Bray, Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 8259, DOI 10.17487/RFC8259, December 2017, https://www.rfc-editor.org/info/rfc8259.

1.4 Informative References

[CPE23-A]

Common Platform Enumeration: Applicability Language Specification Version 2.3 (NISTIR 7698), D. Waltermire, P. Cichonski, K. Scarfone, Editors, NIST Interagency Report 7698, August 2011, https://dx.doi.org/10.6028/NIST.IR.7698.

[CPE23-D]

Common Platform Enumeration: Dictionary Specification Version 2.3, P. Cichonski, D. Waltermire, K. Scarfone, Editors, NIST Interagency Report 7697, August 2011, https://dx.doi.org/10.6028/NIST.IR.7697.

[CPE23-M]

Common Platform Enumeration: Naming Matching Specification Version 2.3, M. Parmelee, H. Booth, D. Waltermire, K. Scarfone, Editors, NIST Interagency Report 7696, August 2011, https://dx.doi.org/10.6028/NIST.IR.7696.

[CPE23-N]

Common Platform Enumeration: Naming Specification Version 2.3, B. Cheikes, D. Waltermire, K. Scarfone, Editors, NIST Interagency Report 7695, August 2011, https://dx.doi.org/10.6028/NIST.IR.7695.

[CVE]

Common Vulnerability and Exposures (CVE) – The Standard for Information Security Vulnerability Names, MITRE, 1999, https://cve.mitre.org/about/.

[CVE-NF]

Common Vulnerability and Exposures (CVE) – The Standard for Information Security Vulnerability Names - CVE ID Syntax Change, MITRE, January 01, 2014, https://cve.mitre.org/cve/identifiers/syntaxchange.html.

[CVRF-1-1]

The Common Vulnerability Reporting Framework (CVRF) Version 1.1, M. Schiffman, Editor, May 2012, Internet Consortium for Advancement of Security on the Internet (ICASI), https://www.icasi.org/the-common-vulnerability-reporting-framework-cvrf-v1-1/.

[CVRF-v1.2]

CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2. Edited by Stefan Hagen. 13 September 2017. OASIS Committee Specification 01. https://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html. Latest version: https://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html.

[CVSS2]

A Complete Guide to the Common Vulnerability Scoring System Version 2.0, P. Mell, K. Scarfone, S. Romanosky, Editors, First.org, Inc., June 2007, https://www.first.org/cvss/cvss-v2-guide.pdf.

[CVSS30]

Common Vulnerability Scoring System v3.0: Specification Document, FIRST.Org, Inc., June 2019, https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf.

[CVSS31]

Common Vulnerability Scoring System v3.1: Specification Document, FIRST.Org, Inc., June 2019, https://www.first.org/cvss/v3-1/cvss-v31-

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-2025

© ISO/IEC 2025 – All rights reserved

specification_r1.pdf.

[CWE]

Common Weakness Enumeration (CWE) – A Community-Developed List of Software Weakness Types, MITRE, 2005, http://cwe.mitre.org/about/.

[CYCLONEDX13]

CycloneDX Software Bill-of-Material Specification JSON schema version 1.3, cyclonedx.org, May 2021, https://github.com/CycloneDX/specification/blob/1.3/schema/bom-1.3.schema.json.

[GFMCMARK]

GitHub's fork of cmark, a CommonMark parsing and rendering library and program in C, https://github.com/github/cmark.

[GFMENG]

GitHub Engineering: A formal spec for GitHub Flavored Markdown, https://githubengineering.com/a-formal-spec-for-github-markdown/.

[ISO8601]

Data elements and interchange formats — Information interchange — Representation of dates and times, International Standard, ISO 8601:2004(E), December 1, 2004, https://www.iso.org/standard/40874.html.

[ISO19770-2]

Information technology — IT asset management — Part 2: Software identification tag, International Standard, ISO 19770-2:2015, September 30, 2015, https://www.iso.org/standard/65666.html.

[ISO29147]

Information technology — Security techniques — Vulnerability disclosure, International Standard, ISO/IEC 29147:2018, October, 2018, https://www.iso.org/standard/72311.html.

[OPENSSL]

GTLS/SSL and crypto library, OpenSSL Software Foundation, https://www.openssl.org/.

[PURL]

Package URL (PURL), GitHub Project, https://github.com/package-url/purl-spec.

[RFC3339]

Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, https://www.rfc-editor.org/info/rfc3339.

[RFC3552]

Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, https://www.rfc-editor.org/info/rfc3552.

[RFC3986]

Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, https://www.rfc-editor.org/info/rfc3986.

[RFC4880]

Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, https://www.rfc-editor.org/info/rfc4880.

[RFC7231]

Fielding, R., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, https://www.rfc-editor.org/info/rfc7231.

[RFC7464]

N. Williams., "JavaScript Object Notation (JSON) Text Sequences", RFC 7464, DOI 10.17487/RFC7464, February 2015, https://www.rfc-editor.org/info/rfc7464.

[RFC8615]

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/64472feb-9402-4c1f-940c-8dd5579a128b/iso-iec-20153-2025

© ISO/IEC 2025 – All rights reserved

Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, https://www.rfc-editor.org/info/rfc8615.

[RFC9116]

Foudil, E. and Y. Shafranovich, "A File Format to Aid in Security Vulnerability Disclosure", RFC 9116, DOI 10.17487/RFC9116, April 2022, https://www.rfc-editor.org/info/rfc9116.

[SCAP12]

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, D. Waltermire, S. Quinn, K. Scarfone, A. Halbardier, Editors, NIST Spec. Publ. 800-126 rev. 2, September 2011, https://dx.doi.org/10.6028/NIST.SP.800-126r2.

[SECURITY-TXT]

Foudil, E. and Shafranovich, Y., *Security.txt Project*, https://securitytxt.org/.

[SemVer]

Semantic Versioning 2.0.0, T. Preston-Werner, June 2013, https://semver.org/.

[SPDX22]

The Software Package Data Exchange (SPDX®) Specification Version 2.2, Linux Foundation and its Contributors, 2020, https://spdx.github.io/spdx-spec/.

[VERS]

vers: a mostly universal version range specifier, Part of the PURL GitHub Project, https://github.com/package-url/purl-spec/blob/version-range-spec/VERSION-RANGE-SPEC.rst.

[VEX]

Vulnerability-Exploitability eXchange (VEX) - An Overview, VEX sub-group of the Framing Working Group in the NTIA SBOM initiative, 27 September 2021, https://ntia.gov/files/ntia/publications/vex_one-page_summary.pdf.

[VEX-Justification]

Vulnerability Exploitability eXchange (VEX) - Status Justifications, VEX sub-group of the Framing Working Group in the CISA SBOM initiative, XX May 2022, https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf.

[XML]

Extensible Markup Language (XML) 1.0 (Fifth Edition), T. Bray, J. Paoli, M. Sperberg-McQueen, E. Maler, F. Yergeau, Editors, W3C Recommendation, November 26, 2008, https://www.w3.org/TR/2008/REC-xml-20081126/. Latest version available at https://www.w3.org/TR/xml.

[XML-Schema-1]

W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures, S. Gao, M. Sperberg-McQueen, H. Thompson, N. Mendelsohn, D. Beech, M. Maloney, Editors, W3C Recommendation, April 5, 2012, https://www.w3.org/TR/2012/REC-xmlschema11-1-20120405/. Latest version available at https://www.w3.org/TR/xmlschema11-1/.

[XML-Schema-2]

W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes, D. Peterson, S. Gao, A. Malhotra, M. Sperberg-McQueen, H. Thompson, Paul V. Biron, Editors, W3C Recommendation, April 5, 2012, https://www.w3.org/TR/2012/REC-xmlschema11-2-20120405/. Latest version available at https://www.w3.org/TR/xmlschema11-2/.

1.5 Typographical Conventions

Keywords defined by this specification use this `monospaced` font.

```
Normative source code uses this paragraph style.
```

Some sections of this specification are illustrated with non-normative examples introduced with "Example" or "Examples" like so:

Examples 4321:

```
Informative examples also use this paragraph style but preceded by the text "Example(s)".
```

iTeh Standards (https://standards.iteh.ai) Document Preview
ISO/IEC 20153:2025
https://standards.iteh.ai/catalog/standards/iso/...8b/iso-iec-20153-2025

© ISO/IEC 2025 – All rights reserved