What’s New in CSAF v2.1?

June 27th 2025

Justin Murphy
CISA

Thomas Schmidt
BSI

Federal Office
for Information Security

TLP:CLEAR

Who are we?

Thomas Schmidt

Technical ICS Analyst @BSI

Passion for:

- ICS
- International Cooperation
- CVD
- Capacity building
- CSAF

Justin Murphy

Vulnerability Analyst @ CISA

Passion for:

- CSAF/OpenEoX
- CVD
- SBOM/VEX
- International Cooperation

Federal Office
for Information Security

TLP:CLEAR

OASIS Open

CSAF

- International, open and free OASIS standard
- Machine-readable format for security advisories (JSON) and VEX
- Standardized way for distribution of security advisories
- Built with automation in mind
- Standardized tool set
- Guidance to actionable information

https://www.csaf.io

Federal Office
for Information Security

TLP:CLEAR

Brief History of CSAF

CVRF
CSAF
CSAF

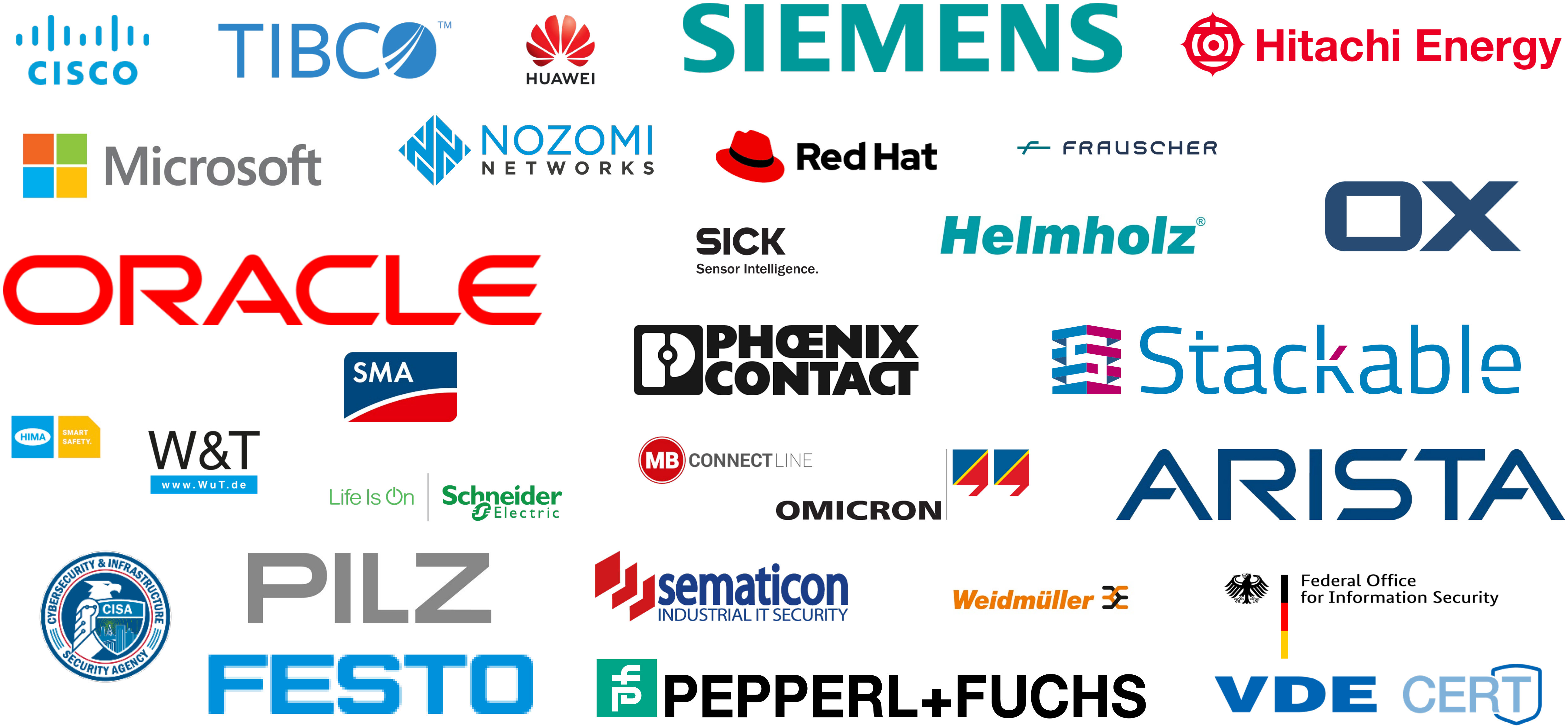
CVRF v1.2

CSAF v2.0

CSAF v2.1

Federal Office
for Information Security

Organizations Publishing CSAF



CSAF Highlights

CSAF v2.0 has been officially recognized as an ISO/IEC standard (ISO/IEC 20153:2025), further solidifying its role in global cybersecurity practices.

CSAF v2.1 CSD01 is now available for public review and comment.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Federal Office
for Information Security

TLP:CLEAR

What’s New in CSAF v2.1?: Key Updates

CVSS v4.0

Metrics vs Scores

CSAF v2.1:

- Replaces the `scores` property with `metrics`.
- Each `metric` item now contains a `content` object that can reference multiple scoring systems including:
  - **CVSS v4**
  - **SSVC v1**
  - **EPSS**
  - CVSS v2, v3
- The `metric` item also includes `products` and an optional `source`.

CSAF v2.0:

- Uses a `scores` array where each score item primarily references CVSS v2 and CVSS v3 alongside the list of products.

TLP 2.0

Traffic Light Protocol (TLP) Labels

In CSAF v2.1, the TLP `label` enumeration has been revised to switch to definitions from TLP v2.0:

- TLP:RED
- TLP:AMBER+STRICT
- TLP:AMBER
- TLP:GREEN
- TLP:CLEAR

In CSAF v2.0, the TLP `label` enumeration is based on TLP v1.0:

- TLP:RED
- TLP:AMBER
- TLP:GREEN
- TLP:WHITE

Vulnerability Property

CWEs

CSAF v2.1:

- The vulnerability object now uses the property `cwes` (plural) instead of a singular `cwe`.
- It is defined as an array where each CWE object must include the fields `id`, `name`, and an additional `version` field.
- Allows multiple weaknesses to be listed and adds specificity with versioning.

CSAF v2.0:

- Vulnerabilities are represented with a single `cwe` object (not an array) and requires only `id` and `name`.

Vulnerability Disclosure and Exploitation

CSAF v2.1:

- Uses `disclosure_date` to indicate when the vulnerability was disclosed to the public.
- Allows for `first_known_exploitation_date` to indicate when the vulnerability was known to be exploited in a specific product.

CSAF v2.0:

- Uses `release_date` instead of `disclosure_date`.

Remediation Enhancements

CSAF v2.1:

- In the `remediations` property, the `category` enumeration has been expanded to include new values:
  - `fix_planned`
  - `optional_patch`
- The other values such as `mitigation`, `no_fix_planned`, `none_available`, and `vendor_fix` remain.

CSAF v2.0:

- The enumeration for remediation categories is limited to `mitigation`, `no_fix_planned`, `none_available`, and `vendor_fix`, and `workaround`.

Product Identification Helper

Package URLs (purls)

CSAF v2.1:

- The field has been renamed from `purl` to `purls` and its type changed from a single string to an array of strings, enabling the listing of multiple package URLs for a product.

CSAF v2.0:

- A singular `purl` field (a string) is used for representing the package URL.

Document Property

Distribution & Sharing

Distribution Object

- In CSAF 2.1, the `distribution` property is now mandatory
- In CSAF 2.0, the `distribution` property is optional.

New Sharing Group

- CSAF 2.1 introduces an optional `sharing_group` within `distribution`.
- An `id` is required and may include a human-readable `name`.

Publisher Object

Additional Category Value:

- In CSAF v2.1 the `` `publisher` `` object's `` `category` `` enumeration has been expanded to include `` `multiplier` ``.
- This new category was not available in CSAF v2.0, which included: `` `coordinator` ``, `` `discoverer` ``, `` `other` ``, `` `translator` ``, `` `user` ``, and `` `vendor` ``.

Schema Property

Schema Identity and Required Properties

CSAF Provider v2.1:

- Declares a `` `$schema` `` property pointing to the v2.1 URL (aka `` `$id` `` of JSON schema).
- `` `$schema` `` property required.

CSAF Provider v2.0:

- JSON schema has an `` `$id` `` pointing to the v2.0 URL, but the instances have no `` `$schema` `` property.

Profiles

Additional Profiles

CSAF v2.1:

- Profile 1 – 5
  - Updates to mandatory fields
- Additional Profiles:
  - Profile 6: Deprecated Security Advisory
  - Profile 7: Withdrawn
  - Profile 8: Superseded

CSAF v2.0:

- Profile 1: CSAF Base
- Profile 2: Security Incident Response
- Profile 3: Informational Advisory
- Profile 4: Security Advisory
- Profile 5: VEX

Tests, Requirements, and Conformance Targets

Additional Changes

- Additions/modifications to:
  - Mandatory, recommended, and informational tests
    - Note: “Optional Tests” (v.2.0) changed to “Recommended Tests”
    - Test presets
  - Distribution Requirements
  - Conformance targets
    - CSAF 2.0 to CSAF 2.1 converter
- Transition process between CSAF 2.0 and CSAF 2.1

Various Housekeeping Items

Directory-based Distribution

CSAF Provider v2.1:

- The distribution mechanism for directory-based distribution is encapsulated as an object under the property `directory`.
- This object requires:
  - `tlp_label` - its value is obtained via a reference to the CSAF v2.1 document's TLP label definition.
  - `url` - the base URL for the directory.

CSAF Provider v2.0:

- The directory distribution is provided as a single property `directory_url`.

ROLIE Distribution

In CSAF v2.1:

- The ROLIE object requires a `feed` array where each feed object must include `last_updated`, `tlp_label`, and `url`.
- The `tlp_label` is referenced from the CSAF v2.1 document schema.

In CSAF v2.0:

- The corresponding ROLIE object requires `feeds` where each feed object requires `tlp_label` and `url` (note the absence of a `last_updated` requirement.)
- The enumeration for `tlp_label` in v2.0 is hardcoded to values from the old version of the TLP protocol.

Public OpenPGP Keys

CSAF Provider v2.1:

- The `public_openpgp_keys` array requires each key object to include both `fingerprint` and `url`.
- The `fingerprint` must meet a minimum length and a pattern (hexadecimal, at least 40 characters).

CSAF Provider v2.0:

- The similar array requires only the `url` property (with `fingerprint` being optional if present.)

Call to Action

CSAF v2.1 CSD01 is now available for public review and comment.

Public review ends July 6, 2025 23:59 UTC.

https://groups.oasis-open.org/discussion/invitation-to-comment-on-csaf-v21-csd01

CSAF Community Days 2025

- Date: November 2025 (calendar week 46)
- Place: TBD (mostly likely in Germany)
- Audience:
  - Tool producers, CSAF issuing, consuming and aggregating parties, National CERTs, ISACs, and industry associations.
- Unique opportunity to learn and share about:
  - Updates for the standard (e.g. CSAF v2.1), tools (available and new), success stories, lessons learned.
- In person participation encouraged/recommended
- Call for presentations soon

Q&A