



What is new in CSAF 2.1

The Future is an Unknown Place

<https://github.com/oasis-tcs/csaf/issues/838>

Agenda

Present

- 01
- Who
 - In Scope
 - Out of Scope

History

- 02
- CVRF 1.2
 - CSAF 2.0
 - CSAF 2.1

Future

- 03
- Created
 - Updated
 - Deleted



P R E S E N T

Security



Who?

Stefan Hagen

Physicist from Bonn

OASIS Distinguished Contributor

Co-author of the GeoJSON format RFC

Passionate about creating actionable standards
CSAF, CVRF, DSS, MQTT, OData, SAM, and SARIF

Software engineer in a Swiss aircraft factory

Why CSAF? In Scope ...

Security Advisories
should provide
actionable advice

Mitigating actions
should be automated to
a high degree

Human administrators
are not always available

Optimize mapping from
vulnerable software to
inventories



Indicators of
Compromise

Stix & Stones

...

Attack detection and mitigation

Vulnerability
enumeration

... Out of Scope

CYBER SECURITY



A S H O R T H i s t o r y

F r o m C V R F t o C S A F

How did we end up here?

- CVRF 1.2
- CSAF 2.0
- CSAF 2.1

Why Change? CVRF - Beginnings

CVRF 1.1 from ICASI
contributed to OASIS

OASIS CVRF 1.2

Created CVSS 3 element

Data modelling language
still XML Schema ...

Updated timestamps
element

“Real” formal spec with
conformance statements



Changed data
modelling language
from XML to JSON
Schema

Added extra layer of
validation via domain
specific rules written down
in the prose

- JSON format with schema (well, 3 files)
- Better product identification (inventory matchers)
- Better vulnerability description (CVSS schema)
- Formulation of distribution scopes (TLP)
- Definition of roles & profiles
- Provision of test suite data
- Specification of distribution channels
- Specification of discovery mechanisms
- Guidance on maximal sizes (taxonomy)

... because everyone
and their dog went the
JSON way, we ...

Stricter data to support
automation and thus ...

... dropped XML
support – no separate
information modelling

... accelerate exchange of
actionable security advice

CSAF 2.0



CYBER SECURITY

A scenic landscape featuring rolling green hills in the foreground, a vibrant rainbow arching across the sky, and rugged mountains in the background. The scene is bathed in the warm, golden light of late afternoon or early morning. A small wooden cabin is visible on a hill to the right, and a dirt path winds through the grass. The overall mood is peaceful and majestic.

D O N E A I I S e t

World already moved on

We did version 2.0! ... Unicorn? Gold Standard?

Why Change? CSAF 2.1

CSAF 2.1 not done yet

Created openly on GitHub:

- prose, schema, test
- tracked issues
- public peer reviews

Many capabilities planned, but some require a CSAF 3.0

<https://github.com/oasis-tcs/csaf> ←

Added or changed capabilities requested from community

The world moved on:

- CVSS 4.0
- TLP 2.0

About 70 issues tagged with 2.1 / 2.x

Shift of perspectives:

- EPSS (prognostics)
- SSVC (stakeholder)

Around 40 issues implemented in 2.1 editor draft already

Cf. Issue #838 for changes from prior version (proposal for new section 1.1)



3a

- # 3b

- cwe → cwes
- distribution
- scores → metrics
- tlp
- version

- n/a

Schema[*]

Identification of schema
is hard

Version "number"

Chicken and egg to
resolve that reference

Added \$schema

- Numbers are implicit
- A URI is explicit



Schema[provider]

Sync within distribution:

- 'directory_url' → 'directory'
- created 'tlp_label' (both members now *\$refs*)
- created 'url'

In 'public_openpgp_keys':

- Changed 'fingerprint' to be required

Migration example:

1. Rename key from 'directory_url' to 'directory'
2. Add key 'tlp_label' to 'directory' value
3. Identify new value for TLP
4. Add value for 'tlp_label' member



`'/vulnerabilities[]/remediations[]/categories':`

- `'fix_planned'`
- `'optional_patch'`

`'/distribution/tlp/label':`

- `'AMBER+STRICT'`
- `'CLEAR'`

`'branch/category':`

- `'platform'`

`'/document/publisher/category':`

- `'multiplier'`

Note: Added `default value`
(`'CLEAR'`) on
`'/distribution/tlp/label'`

Added enum values



CYBER SECURITY

Sharing Groups (Optional)

Added '/distribution/sharing_group' with:

- 'id' of type lowercase UUID (mandatory)
- 'name' (optional)

'id' **SHOULD NOT** change across **different CSAF documents** for the **same sharing group**. It **MUST** differ if a **different sharing group** is addressed. It **MAY** be used by **different issuing parties** to share CSAF documents during a **multi-party coordinated vulnerability disclosure** case.



For any closed sharing group, 'id' SHALL be a UUID4.

A 'TLP:CLEAR' CSAF document **SHOULD NOT** contain a sharing group.

Example values for : '/distribution/sharing_group/id'

- '00000000-0000-0000-0000-000000000000'
- → MAY use to indicate NO_SHARE
- 'f437657f-7076-4c5b-bdbb-0fb592223274'
- → Some closed sharing group
- 'ffffffff-ffff-ffff-ffff-fffffffffffffff'
- → MAY use to indicate 'TLP:CLEAR'

Multiple CWEs per
entry possible

Naming versions of
CWEs is mandatory

Migration example:

1. Key rename from 'cwe' to 'cwes'
2. Wrap existing object in array
3. Add 'version' member

CWE → CWES

CYBER SECURITY

DISTRIBUTION

'/document/distribution':

- object is now mandatory
- member 'tlp' is now mandatory too
- Added optional member 'sharing_group'

Diff: If **both** **multiple** values are present, the TLP information SHOULD be preferred as this aids in automation.

The Sharing Group SHALL be interpreted as specification to the TLP information.

Therefore, the Sharing Group MAY also be used to convey special TLP restrictions

(Informal) Note that for such restrictions the Sharing Group Name MUST exist and all participants MUST know the associated Sharing Group IDs to allow for automation.



Rationale: Metrics other than CVSS possible.

Every 'metrics[]' has:

- 'content' (mandatory)
- 'products' (mandatory)
- 'source' (optional)

Migration example:

1. Wrap every 'scores' member in 'metrics' object
2. Rename key 'scores' into 'content'
3. Consider adding a 'cvss_v4' member inside the 'content' value 😊
4. Add a sibling member 'products'
5. If applicable add 'source' member

Notes:

(1) 'products' is an array with 1 or more products to which 'content' applies

(2) A metric object SHOULD reflect the associated product's status

Example: fixed product → CVSS score of 0, or simply no score listed

SCORES → METRICS



TLP (TRAFFIC LIGHT PROTOCOL)

Upstream changes from TLP 2.0

- new semantic value ('AMBER+STRICT')
- white → clear ('CLEAR')

Setting TLP labels is now mandatory for provider and CSAF JSON instance files



TLP: CLEAR

Well, no surprises here,
but ...

New value '2.1'

Migration example:

1. Change version value from '2.0' to '2.1'

... enumeration to fix a
single value feels weird

Ideally just added new
value with implication
for a superset schema

VERSION



CYBER SECURITY

A Possible Future

Deletions

None ... but the changed elements of course can be seen as deletion of the old and creation of the new containers

Security





Watch this space?

W I N T E R B R E A K

Spring is ready for public review of 2.1 CSD01



THANK YOU

The Future is an Unknown Place