The golden 14 rules for a good Security Advisory in CSAF format

A security advisory in CSAF format should be a well formatted and well understandable source of information to make things clear and not to rise a lot of questions. To reach this goal, the following rules should be applied.

Regarding the document subsection of a CSAF document

1. For property *tlp* the TLP *label* should be set to *WHITE* in order to have no limits in distributing the advisory (`document/distribution/tlp/label`).

2. The *summary* of a *revision_history* entry should be used to describe shortly, clearly and human readable what has been changed in regard to the previous revision. This is an enabler for a fast decision whether a new revision matters or not (`document/tracking/revision_history[]/summary`).

3. The assignment of document ids should be consistent throughout an organization. The document id is used to build the filename and uniquely identify the document (`document/tracking/id`). Together with the publisher namespace, it identifies a document globally unique.

4. The filename must follow the rules, defined in the CSAF standard (section 5.1).

5. The canonical URL in *document/references* makes it possible to automatically retrieve the latest version of that CSAF document.

6. The information to identify a publisher of a CSAF document should not be changed during a document lifecycle except they really change (e.g. new company name; `document/publisher`).

Regarding the product_tree subsection of a CSAF document

7. Provide product information as accurate and detailed as possible, using the *product_tree/branches* including th categoriesvendor, product_name and product_version

8. Provide detailed information to enable a user/customer to properly identify a product in use. Use the Product Identification Helpers to convey that information(/product_tree/*/product/product_identification_helper).

9. Separation of hard- and software (firmware). Make clear how to identify the product itself and how to identify the installed software version, currently used by the product. Make use of relationship objects to convey this information.

Regarding the vulnerabilities subsection of a CSAF document

10. Make clear which products are affected and which are „fixed“ or “not affected” (`vulnerabilities[]/product_status`).

11. Provide CVSS V3.1 scores (`vulnerabilities[]/scores[]`)

12. Provide a CVE tracking number (`vulnerabilities[]/cve`)

13. Provide proper information about the mitigation possibilities through `vulnerabilities [] /remediations`. Use e.g. „`no_fixe_planned`“ if a product is end of life and “none_available” if the fix is currently being developed.

14. A vulnerability should have at least a short summary which could be used for a summary (`vulnerabilities [] /notes`). This ca be the CVE description (category “description”) or a Vulnerability summary (category “summary”).