Federal Office
for Information Security

Technical Guideline TR-03191: Common Security Advisory Framework (CSAF)

Document history

Version	*Date*	*Editor*	*Description*
1.0	2024-05-07	BSI	Initial version
1.0.1	2024-05-27	BSI	Editorial improvements, i.e. no change in normative content

Table 1: Document History

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
E-Mail: csaf@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction

Neither software nor hardware is immune to vulnerabilities. They are flawed as soon as they reach a certain level of complexity. These flaws potentially lead to security vulnerabilities that can be exploited. Vulnerability management is therefore one of the most important tasks for any organisation. As information technology becomes more interconnected and complex, the number of security vulnerabilities steadily increases, thus making manual vulnerability management tedious.

Vulnerabilities and their associated remediation and mitigation measures are typically communicated in the form of security advisories. Today, almost every party issuing security advisories uses its own format, structure and distribution mechanism. As a result, the collection and evaluation of security information is time consuming and resource-intense. In addition, most security advisories are only human-readable, not machine-readable. To speed up the collection and assessment process, automation is key and enables timely action based on available security information.

The Common Security Advisory Framework (CSAF)[1] is an international framework for the communication and automated distribution of machine-processable security information. It is published as an open standard by OASIS Open, originally in November 2022. CSAF significantly reduces the manual effort required to acquire security information and determine whether or not IT-products are affected. CSAF utilises JSON documents which enable organisations to automate the consumption and comparison of security information against a database of IT-assets or Software Bills of Materials (SBOMs). This assessment process is dramatically accelerated, hence allowing organisations to focus on managing risks and remediating vulnerabilities by freeing resources from handling security information.

[1] https://csaf.io/

2 Requirements Language

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119[2].

[2] https://www.rfc-editor.org/info/rfc2119

3 Version of the CSAF standard

The following versions of the CSAF standard as an OASIS Standard SHALL be used to be compliant with this technical guidance:

- CSAF version 2.0 and higher

Errata to a standard MUST be applied if existent.

For higher than the aforementioned minimal version: Only versions with the status “OASIS standard” (“OS”) MUST be used.
Any “Committee Specification Draft” MUST NOT be used.

4 Requirements

4.1 Scope of application

Unless otherwise defined, this technical guidance document applies to all products, services and offerings of an entity that wants or is required to conform to the technical guidance. All items in scope are, in conformance with the CSAF standard, hereafter called products.

4.2 General

If one or more security vulnerabilities are found in a product, then

- CVE[3] numbers for all vulnerabilities MUST be registered and published (including calculation and presentation of the CVSS) and
- Information on the vulnerabilities themselves as well as mitigating measures, including the remediation, MUST be published as a machine-readable security advisory in accordance with the CSAF profiles "Security Advisory" or "VEX" (Vulnerability Exploitability eXchange). As part of the notification, in addition to the affected product versions, the product versions that fix the vulnerability, up to at most the latest available version, MUST also be explicitly stated.

4.3 Document

A CSAF document MUST contain its TLP classification in the specified field **label** to be compliant with this technical guidance. The default SHOULD be TLP:WHITE or TLP:CLEAR depending on the version of the CSAF standard.

4.4 Product tree

The following applies to all CSAF product trees: Individual versions must be enumerated where appropriate. The individual product versions must be specified in such a way that they can be automatically compared with an inventory or asset database. For this purpose, at least the hierarchical structure **vendor/product_name/product_version** MUST be used in the product tree. If an SBOM is mandatory, the hash values of the primary components MUST also be specified in the **product_identification_helper** in accordance with BSI TR-03183-2 for SBOMs. If a product includes hardware, the hardware and software MUST first be listed separately in the product tree and labelled with the relevant **product_identification_helper** (e.g. for hardware: serial number, model number, order number or similar; e.g. for software: SBOM URLs, hash values, etc.). The two are then related to each other via the appropriate **relationship** (usually **installed_on**). The resulting product is then to be used in the **vulnerabilities** section as an overall product comprising hardware and software that are related to each other. This also applies for combinations of firmware and hardware as well as application software and operating systems. Version ranges are allowed only and only if the enumeration of versions is not possible or not reasonable; this is specifically the case for "datetimes", unknown previous version and more than 1,000 versions which would have to be listed. The rules of the CSAF standard apply, including the "no-space-rule", which prohibits the use of whitespace between the comparator and a version, regardless whether a business level test exists or not.

[3] https://www.cve.org/

4.5 Usage of profiles

The CSAF standard defines multiple profiles. If an IT security incident is detected at an entity that wants or is required to conform to the technical guidance or one of its suppliers, corresponding information MUST be provided in accordance with the CSAF “Security Incident Response” profile.

The CSAF profile “Informational Advisory” MUST be used to inform about a misconfiguration which occurred more than just in an individual case.

For vulnerabilities for which the BSI publishes a warning or information with a threat level of orange or red, a “VEX” (see above) MUST be published without undue delay, but not later than 48 hours after the BSI published its text, in accordance with the corresponding CSAF profile, in which the status of the product is listed. The status **under_investigation** is explicitly permitted. This CSAF document MUST be publicly provided, labelled as TLP:WHITE or TLP:CLEAR in accordance with the standard. Other statutory or contractual obligations remain unaffected.

The analysis for any product listed as **under_investigation** MUST conducted in a timely manner.

4.6 Distribution

All CSAF documents MUST be provided in compliance with the CSAF trusted provider role. ROLIE[4] feeds according to the CSAF standard SHOULD be used. Unless otherwise agreed, the documents MUST be made publicly available. Regardless of whether or not user authentication is required due to the classification, the providing party MUST ensure that all authorised users can retrieve all their CSAF documents automatically. For user authentications, at least one of the authentication mechanisms implemented by the reference implementation MUST be supported.

Cryptographic signatures MUST be valid at any given date for more than 30 days. Such signatures SHOULD be valid at any given date for more than 90 days. Signing an old CSAF document just ensures the correct and secure retrieval.

CSAF trusted providers MUST NOT alter the content of any CSAF document without changing its **current_release_date** and updating its **revision_history**. Consequently, CSAF consumers MUST NOT expect new information in the content of a CSAF document as long as the **current_release_date** was not changed.

[4] Resource-Oriented Lightweight Exchange: https://www.rfc-editor.org/info/rfc8322