Joint Interpretation Library

Coordinated Vulnerability Disclosure and Handling Processes

Version 1.0
October 2020

Table of contents

1 Introduction

1 Vulnerability disclosure has long been an open, important issue in cybersecurity.

2 The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet finding vulnerabilities almost every day. This fact is also applicable for evaluated products where, despite a good vulnerability analysis has been done as new techniques or attacks methods are discovered new exploitable vulnerabilities may arise.

3 Other times, due to the implicit characteristics of vulnerability analysis some vulnerabilities may go unnoticed and be discovered later by researchers.

4 The Flaw Remediation Procedures assurance activities in Common Criteria (ALC_FLR) require developers to provide procedures to report, receive and track security flaws and Certification Bodies may sometimes be aware of the existence of new discovered vulnerabilities in certified products. However, there is no specific guidance describing how to responsibly manage the disclosure of these problems among the different actor in the certification community regardless of the inclusion of ALC_FLR in the scope of the evaluation.

5 The SOG-IS agreement requires mutual understanding and trust between certification bodies, including the endeavour to make available to other Participants all information and documentation relevant to the application of the Arrangement.

6 There are different cases where one product may include some other certified product within a certification process:

a) Many products are complex systems that include other third parties' components (e.g. Crypto IP, COTS, etc..).

b) Products can use source code from other products, software libraries, or other types of interfaces.

c) Some products are substantially similar but sold under different brands by different vendors.

d) Different products that support the same network protocol or file format may be affected by a vulnerability in the protocol or format.

7 These interdependencies are important since products that use or interact with a vulnerable product may also be vulnerable. Examples such as ROCA vulnerability highlight coordination challenges.

8 Moreover, during an evaluation, a lab can find that a vulnerability is caused by a vulnerable certified component or platform which another vendor supplies.

9 A special case that shall be taken into consideration is when a vulnerability is found in a TOE that is used as a Platform for a composite TOE and this case will be developed in this supporting document.

10 Inappropriate disclosure of a vulnerability could not only delay the deployment of the vulnerability resolution but also give attackers hints to exploit it. That is why vulnerability disclosure should be carried out in a timely manner and in a coordinated manner among all stakeholders in the certification community.

11 This document aims to provide a coordinated procedure for sharing information about known vulnerabilities in certified products between the different certification bodies, clearly describing authorized vulnerability disclosure and discovery conduct, thereby substantially reducing the risk for final users.

12 The guidelines provided by the International Organization for Standardization on vulnerability disclosure (ISO 29147, Vulnerability Disclosure) and the NTIA's multi-stakeholder work on vulnerabilities and disclosure has been used as a basis for this document.

2 Roles

13 For the purposes of this document, the following actors are identified:

a) Finder: individual or organization that identifies a potential vulnerability in a certified TOE. It can be an evaluation lab, but it is not limited to, since vulnerabilities may come from independent researchers or other sources. This document does not put the focus on the Finder but in the Issuing CB, as responsible of the certified TOEs.

b) Vulnerable TOE: The evaluated and certified product where the vulnerability has been found.

c) Vulnerable Vendor: The developer of the Vulnerable TOE.

d) Affected TOE: An evaluated and certified product that gets a subsystem from a Vulnerable TOE and uses it to supply a system or service, maybe as part of the environment or as part of the TOE.

e) Affected Vendor: The developer of the Affected TOE.

f) Issuing CB: The SOG-IS Certification Body where the vulnerable TOE was certified.

g) Interested CBs: All the SOG-IS Certification Bodies.

h) Affected CBs: An interested SOG-IS CB that has confirmed that the vulnerability affects a TOE certified by them.

3 Advisory content

14 As part of the Coordinated Vulnerability Disclosure and Handling Process, the Issuing CB shall generate a Security Advisory at most a month after being notified describing the problem found.This document will be referred hereinafter as [ADVISORY]. This document is expected to be updated several times until the vulnerability is considered fixed.

15 This section describes the expected contents of such documents, but it may be tailored by each Issuing Certification Body depending on the vulnerability nature.

a) Unique identifier: It is imperative that the advisory use both a unique numbering and naming convention. The naming convention shall include an identifier of the Issuing CB.

b) References to the certificates of the affected TOE(s).

c) Version: a version number is mandatory

d) Overview: This advisory should provide a summary on the vulnerability first so that everyone can understand the essential points quickly and allows identification of affected TOEs.

e) Description: Full description clearly explaining the vulnerability, specifying the name, the cause, and other available information.

f) Threats: The advisory should provide information about known threats that relate to the vulnerability, (e.g. the existence of exploit or proof-of-concept code, discussion or evidence of incident activity). It may be desirable to list the affected TOE threats specified in the applicable ST.

g) Impact: The advisory should describe potential/expected consequences of attacks against the vulnerability. Attacks can have multiple impacts (e.g. an attack against a buffer overflow vulnerability could cause a crash or execute code). Where possible, describe secondary impacts (e.g. a cross-site scripting vulnerability directly allows an attacker to inject content into a web page; however, the secondary impact can be the exposure of cookies or other authentication credentials).

h) Solution: For product vulnerabilities, the advisory should provide information on how to install the fixed product, update and apply a security patch. If the patch is not yet ready, a tentative schedule must be provided under “Disclosure and Resolution times”.

i) Workarounds: The advisory should provide workaround information if the users can protect the affected products in use through operational effort or by limiting the use of it in some way without applying the security patch.

j) References: If additional information on the vulnerability that the users could refer to is available, the advisory should provide the links as reference. This include other related advisories identifiers, like a CVE-ID number.

k) Vulnerable versions: descriptive list of affected products and versions. This might also include an explanation of how to confirm the version of these products including the vendor nomenclature for naming and numbering.

l) Disclosure and Resolution times: Date for problem resolution and disclosure. Use **7 days** from the date that the CB is aware as a good practice for disclosure and **90 days** for resolution. This document does not put any restriction on this term, except for the duty to meet the agreed dates without exception.

16 Since vulnerability information may be used to attack vulnerable products and online services, sensitive vulnerability information should be communicated confidentially. Message integrity is also important, particularly in verifying that remediation information is authentic. Common cryptographic protocols such as Pretty Good Privacy (PGP) can provide confidentiality and integrity.

4 General Overview of the process

17 Please, note that the involved stakeholders have been previously described in section Roles.

18 The following steps should be followed:

1. The process usually starts when a "Finder" founds a potential vulnerability in a certified TOE. The finder may be a lab, a researcher, or the vendor itself.
2. In order to follow this procedure, the Issuing CB must be notified of the existence of the vulnerability. The Responsible Disclosure process cannot go on until the Issuing CB is notified.
3. When the Issuing CB is aware of the vulnerability, the Issuing CB shall investigate the potential vulnerability and based on this analysis shall decide if further actions are necessary.
4. If further actions are deemed necessary, the Issuing CB should notify the Vulnerable Vendor to confirm the presence of the problem, and ask the vendor for cooperation in the assessment of the potential vulnerability.
5. The Vulnerable Vendor should have the responsibility to assess the problem and if necessary to take actions to cover the problem including contracting an ITSEF.
6. As soon as the potential vulnerability is confirmed by the Issuing CB and/or the vulnerable vendor, a preliminary advisory package has to be developed by the developer in cooperation with the CB and the ITSEF. This document shall be sent to all SOGIS members, including the proposed schedule for Disclosure and Resolution date. Within the scope of the definition of the preliminary advisory package, definition of the confidentiality status shall be provided. The Vulnerable Vendor will provide to the Issuing CB enough information to allow preliminary identification of the Affected TOEs.
7. Following the confidentiality status, the Issuing CB shall request the agreement of the Vulnerable Vendor to disclose the vulnerability presence between all SOGIS members based on Need-to-know principle and confidentiality claim. If the Vulnerable Vendor does not allow the disclosure of the vulnerability to the Interested CBs, the only option to proceed is for the Issuing CB is to withdraw the certificate of the affected TOEs.The Issuing CB will broadcast this preliminary advisory package to the Interested CBs (all SOGIS members) not later than **7 days** since the Issuing CB has received the confirmation of the Vulnerable Vendor.
8. A time of **7 days** is given to the Interested CBs to notify the presence of an Affected TOE between their certified products to the Issuing CB. The Interested Certification Bodies with Affected TOEs are called from now on Affected Certification Bodies.
9. The Vulnerable Vendor should notify also within a time period of **7 days** to the affected vendors that may include the vulnerable TOE within its certified TOE.

10. The Vulnerable Vendor in cooperation with the Issuing CB should continue with incident handling procedure to solve the vulnerability. During this period if relevant information, such as partial vulnerability mitigations, identification of some other Affected TOEs, etc., the Issuing CB and/or the Vulnerable Vendor shall update the preliminary advisory package, and shall notify Affected CBs to take proper actions as soon as possible.
11. After completion of the full investigation and incident resolution is performed (i.e. fixing the problem or providing a patch), the Issuing CB in cooperation with the Vulnerable Vendor will create the final advisory package [ADVISORY], including the list of the Affected TOEs and the proposed resolution of the vulnerability. A time of **7 days** is recommended to deliver the document to Affected CBs by the Issuing CB.
12. The final advisory [ADVISORY] is now sent by the Vulnerable Vendor to the Affected Vendors, the manufacturers of the Affected TOEs, by the Affected CBs.
13. When the date of the disclosure arrives, the Issuing CB is allowed to make public a trimmed version of the advisory without the details of the vulnerability.

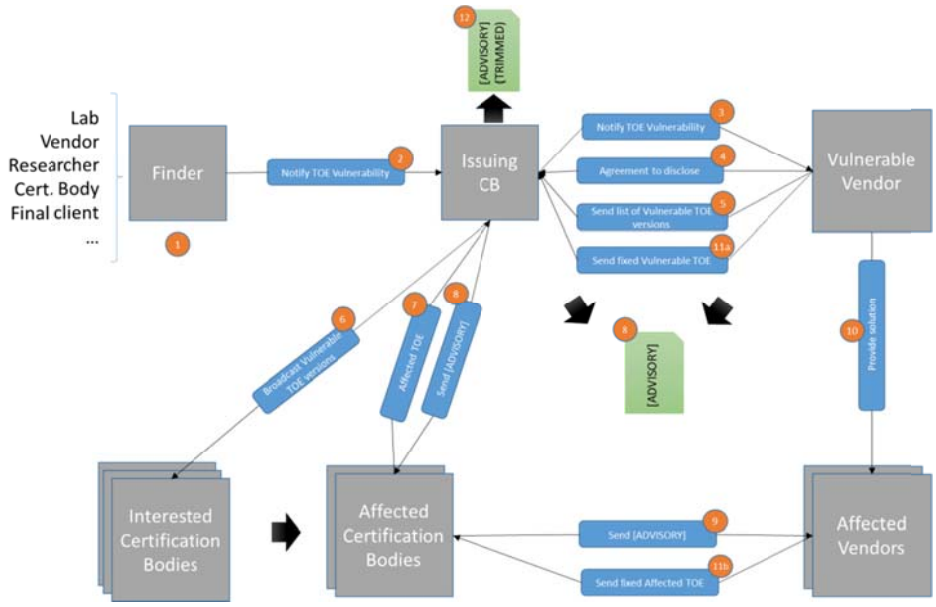

Figure 1- To be updated after process approval

19 The way of broadcasting preliminary advisory or final advisory document depends on urgency and confidentiality of the problem. The defined time periods in the above steps are considered as good practice in case critical vulnerabilities are identified.

20 This document does not restrict other communication flows that may occur between the parties, particularly between Affected CBs and Affected Vendors or between Affected and Vulnerable Vendors.

21 Finally, the advisory document by the Issuing CB is expected to be updated at any time significant changes to solve the vulnerability are achieved.

5 References

- The NTIA's multi-stakeholder work on vulnerabilities and disclosure available athttps://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
- The International Organization for Standardization's guidance on vulnerability disclosure (ISO 29147, Vulnerability Disclosure) available for free at http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip