TECHNICAL REPORT

ISO/IEC TR 20004

Second edition
2015-12-15

Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

Technologies de l'information — Techniques de sécurité — Redéfinition de l'analyse de vulnérabilité de logiciel selon l'ISO/CEI 15408 et l'ISO/CEI 18045

Reference number
ISO/IEC TR 20004:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Terms and definitions **1**

3 Abbreviated terms **3**

4 Background context **4**

5 Vulnerability assessment activities **8**

5.1 Determine relevant potential vulnerabilities 9

5.1.1 Identify relevant weaknesses and attack patterns from existing structured assurance case 11

5.1.2 Identify relevant weaknesses and attack patterns from public sources 11

5.2 Assess TOE susceptibility to attack 14

5.2.1 Design and specify security/penetration testing 14

5.2.2 Execute and document security/penetration testing 15

5.3 Report on exploitable vulnerabilities 15

Bibliography **17**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC/TR 20004:2012), which has been technically revised.

Introduction

This Technical Report is intended to provide added refinement, detail and guidance to the vulnerability analysis activities outlined in ISO/IEC 18045:2008 for the software elements of a TOE. Specifically, it is intended to add refinement and clarification of the “Potential vulnerability identification from public sources” (AVA_VAN.1.2E/2.2E/3.2E/4.2E) and “Penetration testing” (AVA_VAN.1.3E/2.4E/3.4E/4.4E) evaluator actions, which are currently imprecise in regards to searching for, identifying and testing relevant potential vulnerabilities. This Technical Report provides guidance on an approach to objectively search for, identify, filter and test potential vulnerabilities utilizing international ad hoc standard resources for software weaknesses and attack patterns. The set of relevant software weaknesses and attack patterns identified through this guidance represent a minimal set for analysis under the AVA_VAN assurance family in an ISO/IEC 15408 evaluation. Additional weaknesses and attack patterns may be determined relevant by specific national schemes, technical communities, associated protection profiles or other sources. In utilizing these standard structured resources, the approach defined here has the added benefit of being equally applicable to the TOE development process as it does to the TOE security evaluation process. This means that relevant weaknesses and attack patterns identified and tested for during development, whether defined ad hoc or as part of a structured assurance case, can provide a head start template for a TOE-specific set of relevant weaknesses and attack patterns for use in the security evaluation.

This Technical Report is intended to be used in conjunction with and, as an addendum to, ISO/IEC 18045.

This Technical Report does not address all possible vulnerability analysis methods, in particular those that fall outside the scope of the activities outlined in ISO/IEC 18045. It uses the common weakness enumeration (CWE) and the common attack pattern enumeration and classification (CAPEC) to identify possible attacks. It does not preclude the use of other appropriate identification resources by evaluators.

The target audience for this Technical Report is evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions, developers, PP/ST authors (to include Technical Communities), evaluator sponsors and other parties interested in IT security.

This Technical Report recognizes that not all questions concerning IT security evaluation will be answered herein and that further interpretations will be needed. Individual schemes will determine how to handle such interpretations and other guidance, although these can be subject to mutual recognition agreements.

Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

1 Scope

This Technical Report refines the AVA_VAN assurance family activities defined in ISO/IEC 18045 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation. This Technical Report leverages publicly available information security resources to support the method of scoping and implementing ISO/IEC 18045 vulnerability analysis activities. The Technical Report currently uses the common weakness enumeration (CWE) and the common attack pattern enumeration and classification (CAPEC), but does not preclude the use of any other appropriate resources. Furthermore, this Technical Report is not meant to address all possible vulnerability analysis methods, including those that fall outside the scope of the activities outlined in ISO/IEC 18045.

This Technical Report does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
assurance case
structured set of claims, arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties

2.2
attack pattern
abstracted approach utilized to attack software

2.3
attack potential
measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation

[SOURCE: ISO/IEC 15408-1:2009, 3.1.5]

2.4
confirm
declare that something has been reviewed in detail with an independent determination of sufficiency

Note 1 to entry: The level of rigour required depends on the nature of the subject matter. This term is only applied to evaluator actions.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.14]

2.5
CVE vulnerability
vulnerability listed in CVE

2.6
determine
affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms “confirm” or “verify” which imply that an analysis has already been performed which needs to be reviewed.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.22]

2.7
encountered potential vulnerabilities
potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs

[SOURCE: ISO/IEC 15408-1:2009, 3.5.2]

2.8
evaluation
assessment of a PP, an ST or a TOE, against defined criteria

[SOURCE: ISO/IEC 15408-1:2009, 3.1.26]

2.9
exploitable vulnerability
weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE

[SOURCE: ISO/IEC 15408-1:2009, 3.5.3]

2.10
potential vulnerability
suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the SFRs.

[SOURCE: ISO/IEC 15408-1:2009, 3.5.5]

2.11
Protection Profile
implementation-independent statement of security needs for a TOE type

[SOURCE: ISO/IEC 15408-1:2009, 3.1.52]

2.12
residual vulnerability
weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE

[SOURCE: ISO/IEC 15408-1:2009, 3.5.6]

2.13
Security Target
implementation-dependent statement of security needs for a specific identified TOE

[SOURCE: ISO/IEC 15408-1:2009, 3.1.63]

2.14
selection
specification of one or more items from a list

[SOURCE: ISO/IEC 15408-1:2009, 3.1.64]

2.15
target of evaluation
set of software, firmware and/or hardware possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, 3.1.70]

2.16
threat agent
entity that can adversely act on assets

[SOURCE: ISO/IEC 15408-1:2009, 3.1.71]

2.17
TOE evaluation
assessment of a TOE against defined criteria

[SOURCE: ISO/IEC 15408-1:2009, 3.1.72]

2.18
TOE-relevant CVE vulnerabilities
CVE vulnerabilities from all versions of the TOE product family or CVE vulnerabilities associated with products of the same technology type

2.19
verify
rigorously review in detail with an independent determination of sufficiency

Note 1 to entry: Also see *confirm* (2.4). The term *verify* has more rigorous connotations. It is used in the context of evaluator actions where an independent effort is required of the evaluator.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.84]

2.20
vulnerability
weakness in the TOE that can be used to violate the SFRs in some environment

[SOURCE: ISO/IEC 15408-1:2009, 3.5.7]

2.21
weakness
characteristic or property of a TOE that, in proper conditions, could contribute to the introduction of vulnerabilities within that TOE

3 Abbreviated terms

The following abbreviations are used in one or more parts of ISO/IEC 20004.

CAPEC™[a]	Common Attack Pattern Enumeration and Classification
CVE®[a]	Common Vulnerabilities and Exposures
CWE™[a]	Common Weakness Enumeration
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

[a] CAPEC, CVE and CWE are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

4 Background context

ISO/IEC 15408-3:2008, 15.1 defines “development vulnerabilities” as vulnerabilities which take advantage of some properties of the TOE which were introduced during its development. In the same sub-clause, ISO/IEC 15408-3 states that an assessment of development vulnerabilities is covered by the assurance family called “vulnerability analysis” (AVA_VAN). ISO/IEC 15408-3 expects this assessment to determine whether potential vulnerabilities identified could allow attackers to violate the SFRs and to deal with the threat that an attacker will be able to discover flaws [as the identified potential vulnerabilities] (ISO/IEC 15408-3:2008, 15.2.1).

The levels in the AVA_VAN assurance family are ordered as follows:

- AVA_VAN.1 “vulnerability survey” (ISO/IEC 15408-3:2008, 15.2.3);
- AVA_VAN.2 “vulnerability analysis” (ISO/IEC 15408-3:2008, 15.2.4);
- AVA_VAN.3 “focused vulnerability analysis” (ISO/IEC 15408-3:2008, 15.2.5);
- AVA_VAN.4 “methodical vulnerability analysis” (ISO/IEC 15408-3:2008, 15.2.6);
- AVA_VAN.5 “advanced methodical vulnerability analysis” (ISO/IEC 15408-3:2008, 15.2.7).

AVA_VAN.1 is the lowest level and AVA_VAN.5 is the highest level in the AVA_VAN assurance family.

ISO/IEC 15408-3 states the following two evaluator actions for each of the AVA_VAN levels.

- “Potential vulnerability identification from public sources” action

  The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

  - AVA_VAN.1.2E (ISO/IEC 15408-3:2008, 15.2.3.4.2);
  - AVA_VAN.2.2E (ISO/IEC 15408-3:2008, 15.2.4.4.2);
  - AVA_VAN.3.2E (ISO/IEC 15408-3:2008, 15.2.5.4.2);
  - AVA_VAN.4.2E (ISO/IEC 15408-3:2008, 15.2.6.4.2);
  - AVA_VAN.5.2E (ISO/IEC 15408-3:2008, 15.2.7.4.2).

- “Penetration testing” action

  The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing.

  - Basic attack potential” in AVA_VAN.1.3E (ISO/IEC 15408-3:2008, 15.2.3.4.3);
  - Basic attack potential” in AVA_VAN.2.4E (ISO/IEC 15408-3:2008, 15.2.4.4.4);

- Enhanced-Basic attack potential” in AVA_VAN.3.4E (ISO/IEC 15408-3:2008, 15.2.5.4.4);
- Moderate attack potential” in AVA_VAN.4.4E (ISO/IEC 15408-3:2008, 15.2.6.4.4);
- High attack potential” in AVA_VAN.5.4E (ISO/IEC 15408-3:2008, 15.2.7.4.4).

ISO/IEC 18045 further specifies certain work units associated with the “Potential vulnerability identification from public sources” action (in ISO/IEC 18045:2008, 14.2.1.5, 14.2.2.5, 14.2.3.5 and 14.2.4.5) as follows.

- AVA_VAN.1-3, AVA_VAN.2-3, AVA_VAN.3-3, AVA_VAN.4-3

  The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.

The availability of information, that may be readily available to an attacker that helps to identify and facilitate attacks, effectively operates to substantially enhance the attack potential of a given attacker. The accessibility of vulnerability information and sophisticated attack tools on the Internet makes it more likely that this information will be used in attempts to identify potential vulnerabilities in the TOE and exploit them. Modern search tools make such information easily available to the evaluator, and the determination of resistance to published potential vulnerabilities and well known generic attacks can be achieved in a cost-effective manner.

The search of the information publicly available should be focused on those sources that refer specifically to the product from which the TOE is derived. The extensiveness of this search should consider the following factors: TOE type, evaluator experience in this TOE type, expected attack potential and the level of ADV evidence available.

- AVA_VAN.1-4, AVA_VAN.2-5, AVA_VAN.3-5, AVA_VAN.4-5

  The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.

It may be identified that no further consideration of the potential vulnerability is required if, for example, the evaluator identifies that measures in the operational environment, either IT or non-IT, prevent exploitation of the potential vulnerability in that operational environment.

The evaluator records any reasons for exclusion of potential vulnerabilities from further consideration if the evaluator determines that the potential vulnerability is not applicable in the operational environment. Otherwise, the evaluator records the potential vulnerability for further consideration.

A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.

NOTE As stated in ISO/IEC 18045:2008, 14.2.5, ISO/IEC 18045 does not specify any work units at the AVA_VAN.5 level.

The content of the “Potential vulnerability identification from public sources” evaluator action is summarized in the following diagram.