TECHNICAL REPORT

ISO/IEC TR 20004

First edition
2012-08-15

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 20004:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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. 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.

ISO/IEC TR 20004:2012 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction

This Technical Report provides added refinement, detail and guidance to the vulnerability analysis activities outlined in ISO/IEC 18045:2008(E). It is intended to be used in conjunction with and as an addendum to ISO/IEC 18045:2008(E). The refinement, detail and guidance provided by this document are not intended to satisfy the full range of requirements under the AVA_VAN family as defined in ISO/IEC 18045:2008(E) or to artificially restrict the activities performed by evaluators but rather to facilitate consistency through a minimal baseline of AVA_VAN evaluation.

The target audience for this Technical Report is primarily evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions; evaluation sponsors, developers, PP/ST authors and other parties interested in IT security are a secondary audience.

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 18045:2008 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 the Common Weakness Enumeration (CWE) and the Common Attack Pattern Enumeration and Classification (CAPEC) to support the method of scoping and implementing ISO/IEC 18045:2008 vulnerability analysis activities.

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, definition 3.1.5]**

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

NOTE 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, definition 3.1.14]**

2.5
CVE vulnerability
vulnerability listed in CVE