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
Contents

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
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.