TECHNICAL SPECIFICATION

ISO/IEC TS 9569

First edition
2023-11

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des TI — Extension pour la gestion des correctifs concernant la série ISO/IEC 15408 et l'ISO/IEC 18045

Reference number
ISO/IEC TS 9569:2023(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection.*

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 15408 series is intended to be used to evaluate the assurance of IT products. While the ISO/IEC 15408 series can be used to perform an initial evaluation of an IT product, it does not support a differential security evaluation of that product, subsequent to one or several patches being applied to it. Neither the ISO/IEC 15408 series nor ISO/IEC 18045 contain dedicated methods or evaluation activities which would support the evaluation of changes or updates.

Some of these aspects were addressed by users of the ISO/IEC 15408 series, in particular evaluation authorities, but also within the mutual recognition agreements (e.g. Common Criteria Recognition Arrangement). In many real-world use-cases, developers provide updated or patched target of evaluations (TOEs), but the effort to re-certify these versions has mostly been avoided.

This problem of patch management and its related components are missing from the current ISO/IEC 15408 series and ISO/IEC 18045. To address this problem, requirements and recommendations are needed on how to regain assurance of an updated target of evaluation in a standardized and widely accepted way e.g. in terms of effort and costs.

This document collects discussions and experience from the experts involved in the ISO/IEC 15408 series and ISO/IEC 18045, to address the evaluation of the patch management during the evaluation of the initial TOE in a standardized way. This document also discusses alternatives for the evaluation of patched TOEs, although it does not provide a standardized approach.

This document is intended to be used as an extension to the ISO/IEC 15408 series and ISO/IEC 18045.

Clause 5 includes the definition of the new patch management assurance family following the structure defined in the ISO/IEC 15408 series and ISO/IEC 18045. Clause 6 includes additional guidance for the evaluators of the initial target of evaluation (TOE). Annex A summarizes experiences in evaluation schemes as options for adoption.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type. The use of italics indicates text that has a precise meaning. For security assurance requirements, the convention is for special verbs relating to evaluation.

This document follows the conventions introduced in the ISO/IEC 15408 series and ISO/IEC 18045.

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045

1 Scope

This document specifies patch management (PAM) security assurance requirements and is intended to be used as an extension of the ISO/IEC 15408 series and ISO/IEC 18045.

The security assurance requirements specified in this document do not include evaluation or test activities on the final target of evaluation (TOE), but focus on the initial TOE and on the life cycle processes used by manufacturers. Additionally, this document gives guidance to facilitate the evaluation of the TOE, including the patch and development processes which support the patch management.

This document lists options for evaluation authorities (or mutual recognition agreements) on how to utilize the additional assurance and additional evidence in their processes to enable the developer to consistently re-certify their updated or patched TOEs to the benefit of the users. The implementation of these options using an evaluation scheme is out of the scope of this document.

2 Normative references

There are no normative references in this document.