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)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Overview ... **4**
4.1 Background information ... 4
4.2 Proposed approach ... 6
4.3 Non-public vulnerabilities ... 6
5 Patch management family ... **7**
5.1 General ... 7
5.2 Patch management (ALC_PAM) ... 7
5.2.1 Objectives ... 7
5.2.2 Component levelling ... 7
5.2.3 Application notes ... 7
5.2.4 ALC_PAM.1 Patch management ... 8
5.3 Evaluation work units for ALC_PAM ... 9
5.3.1 Action ALC_PAM.1.1E ... 9
6 Additional guidance for evaluators ... **13**
6.1 General ... 13
6.2 Class ASE ... 13
6.2.1 ASE_INT ... 13
6.3 Class ADV ... 14
6.3.1 ADV_ARC ... 14
6.3.2 ADV_FSP ... 14
6.3.3 ADV_IMP ... 14
6.3.4 ADV_TDS ... 14
6.4 Class AGD ... 14
6.4.1 AGD_OPE ... 14
6.4.2 AGD_PRE ... 14
6.5 Class ALC ... 14
6.5.1 ALC_CMC ... 14
6.5.2 ALC_CMS ... 15
6.5.3 ALC_DEL ... 15
6.5.4 ALC_DVS ... 16
6.5.5 ALC_FLR ... 16
6.5.6 ALC_LCD ... 16
6.5.7 ALC_TAT ... 16
6.6 Class ATE ... 17
6.6.1 ATE_COV ... 17
6.6.2 ATE_DPT ... 17
6.6.3 ATE_IND ... 17
6.7 Class AVA ... 17
6.7.1 AVA_VAN ... 17
Annex A (informative) **Options for evaluation authorities** ... **18**
Annex B (informative) **Template for the security relevance report** ... **21**
Annex C (informative) **ALC_PAM PMD examples** ... **22**
Annex D (informative) **Patch management functional package example** ... **25**
Bibliography ... **36**

© ISO/IEC 2023 – All rights reserved

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.

© ISO/IEC 2023 – All rights reserved

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.

© ISO/IEC 2023 – All rights reserved

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.

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
activation
operation performed on a patch to transform the *initial target of evaluation (TOE)* (3.8) into the *final TOE* (3.4)

Note 1 to entry: Activation is an atomic operation which can only be done in one step (partial activation is not allowed).

Note 2 to entry: In addition to installing the modified functionality, this operation shall encompass a change in TOE identification.

Note 3 to entry: The TOE shall remain in a secure state even if interruption or incident occurs during such operation, which prevents the forming of the final TOE.

3.2
end-of-support
date until when the user can expect to receive new patches

Note 1 to entry: The end-of-support should be greater than the period of validity of the certificate.

© ISO/IEC 2023 – All rights reserved

Note 2 to entry: The period of validity of the certificate can be extended through the standard assurance continuity.

3.3
evaluation authority
body operating an evaluation scheme

[SOURCE: ISO/IEC 15408-1:2022, 3.40]

3.4
final target of evaluation
final TOE
initial TOE (3.8) with the *patches* (3.11) applied

Note 1 to entry: The final TOE is obtained by combining the initial TOE and patch(es) to be loaded and activated on the initial TOE.

Note 2 to entry: The final TOE is not necessarily evaluated but assurance is gained through ALC_PAM on the initial TOE.

3.5
flaw remediation
assurance family ALC_FLR which provides requirements for the handling of security flaws

Note 1 to entry: This definition of flaw remediation is based on ISO/IEC 15408-3:2022, 12.1.

3.6
identification data
data that identifies the *initial target of evaluation* (3.8), the applied *patch(es)* (3.11) or the *final target of evaluation* (3.4)

3.7
initial evaluation
complete evaluation of the *initial target of evaluation* (3.8)

3.8
initial TOE
initial target of evaluation
target of evaluation (TOE) (3.18) that supports evaluated features allowing at least to securely load, activate and execute patch(es), without any applied patches

Note 1 to entry: The *final TOE* (3.4) is obtained by loading and activating the patches for the initial TOE.

Note 2 to entry: The final TOE may not be evaluated but assurance is gained through the evaluation of ALC_PAM on the initial TOE.

3.9
loader
piece of the *target of evaluation security functionality* (3.19) of the *initial target of evaluation* (3.8) that implements the *activation* (3.1) of a *patch* (3.11)

3.10
maintenance
process provided by an evaluation authority that recognises that a set of one or more applied *patches* (3.11) made to an *initial target of evaluation (TOE)* (3.8) has not adversely affected the assurance

Note 1 to entry: Changes in the development environment can be considered as maintenance if they relate to the TOE.

Note 2 to entry: Maintenance is typically applied in the context of certification.

© ISO/IEC 2023 – All rights reserved

3.11
patch
type of source code or binary code to be added to an *initial target of evaluation (TOE)* (3.8) in order to introduce additions or modifications of a functional or security feature

Note 1 to entry: A patch is loaded on the initial TOE and activated to obtain the final TOE.

Note 2 to entry: Full replacement of a TOE is a possible implementation of "patchability" and a current practice for software TOEs.

3.12
patch management
PAM
processes applied during *patch* (3.11) development and patch release

3.13
patch management documentation
PMD
documentation describing the policies, processes, procedures related to the patching of the *target of evaluation* (3.18)

3.14
patch verification mechanism
technical mechanism to verify the integrity and/or authenticity of a *patch* (3.11)

3.15
re-evaluation
process of recognising that changes made to an *initial target of evaluation* (3.8) require independent evaluator activities to be performed in order to establish a new assurance baseline

Note 1 to entry: Re-evaluation seeks to reuse results from a previous evaluation.

3.16
security assurance requirement
SAR
security requirement that refers to the conditions and processes for the development and delivery of the *target of evaluation* (3.18), and the actions required of evaluators with respect to evidence produced from these conditions and processes

[SOURCE: ISO/IEC 15408-1:2022, 3.76]

3.17
security relevance report
SRR
document containing the assessment of security relevance of a *patch* (3.11)

3.18
target of evaluation
TOE
set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

[SOURCE: ISO/IEC 15408-1:2022, 3.90]

3.19
target of evaluation security functionality
TOE security functionality
TSF
combined functionality of all hardware, software, and firmware of a *target of evaluation (TOE)* (3.18) that is relied upon for the correct enforcement of the security functional requirements

[SOURCE: ISO/IEC 15408-1:2022, 3.92]

© ISO/IEC 2023 – All rights reserved

3.20
transport
process of transferring patches from the developer to the user who applies the *patch* (3.11)

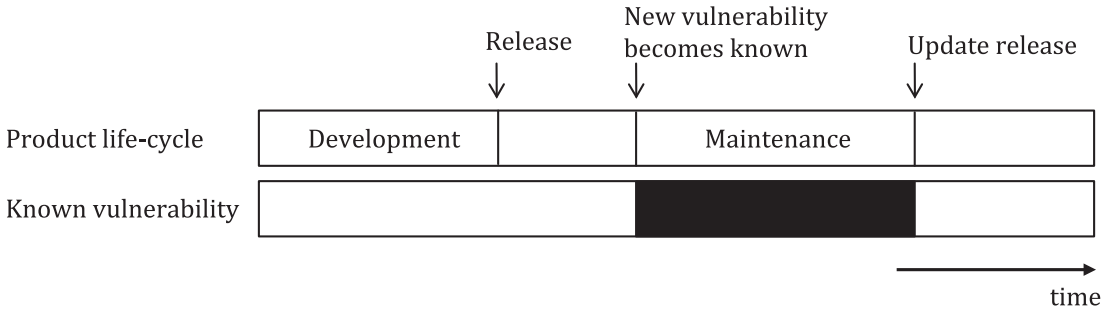
3.21
vulnerability
weakness in the *target of evaluation* (3.18) that can be used to violate the security functional requirements in a specified environment

Note 1 to entry: In the definition of ALC_PAM.1 in 5.2.4, the term flaw is used to ensure consistency with ALC_FLR components.

4 Overview

4.1 Background information

Figure 1 shows the product vulnerability timeline for the case after a new vulnerability is detected and becomes publicly known. Until the developer releases an update that removes the vulnerability, and that update is applied, the product will be insecure. This status is shown in black below.



Key

The product is vulnerable due to the lack of a patch.

Figure 1 — Product vulnerability timeline

Consequently, developers have a responsibility to build and release those updates in a short period of time after the vulnerability becomes known. Developers who obtained a certificate previously may request a re-evaluation of the TOE (for example for issuing a new certificate, or because it is mandated by their clients). In many real-world cases, re-evaluation does not happen for every patch of the product, mostly due to cost and delay.

Since the patched TOE has not been re-evaluated, the developer can introduce a regression defect while deploying the vulnerability fix or in the fix itself. In the absence of evaluation by a skilled third party, there is a general lack of assurance on the patched TOE. This transfers the decision to use either a previously certified or a recently patched version to the user of the TOE.

Therefore, the user of the TOE should run their own risk assessment to determine which version of the TOE to use. If users of the TOE limit themselves to evaluated versions, they therefore accept known vulnerabilities in the TOE. Further risk mitigation should also be done, i.e. additional compensating countermeasures against the new vulnerabilities should be implemented. Conversely, using patched TOEs can also include flaws introduced by the developer during the patch development or deployment.

Figure 2 illustrates the timeline and relationship of a TOE when a new vulnerability occurs, a patch becomes available and the status of the certification is not in sync.

© ISO/IEC 2023 – All rights reserved