FINAL
DRAFT

TECHNICAL SPECIFICATION

ISO/IEC DTS 9569

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-08-16

Voting terminates on:
2023-10-11

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-2d4cd6b20c25/iso-iec-dts-9569

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

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

© ISO/IEC 2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-2d4cd6b20c25/iso-iec-dts-9569

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/...iso-iec-dts-9569

© 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

© 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569

© ISO/IEC 2023 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-2d4cd6b20c25/iso-iec-dts-9569

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 Normative references

There are no normative references in this document.

ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-2d4cd6b20c25/iso-iec-dts-9569

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* (3.5)

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.6
identification data
data that identifies the *initial target of evaluation* (3.8), the applied *patch(es)* (3.13) or the *final target of evaluation* (3.5)

ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-2d4cd6b20c25/iso-iec-dts-9569

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-2d4cd6b20c25/iso-iec-dts-9569

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)

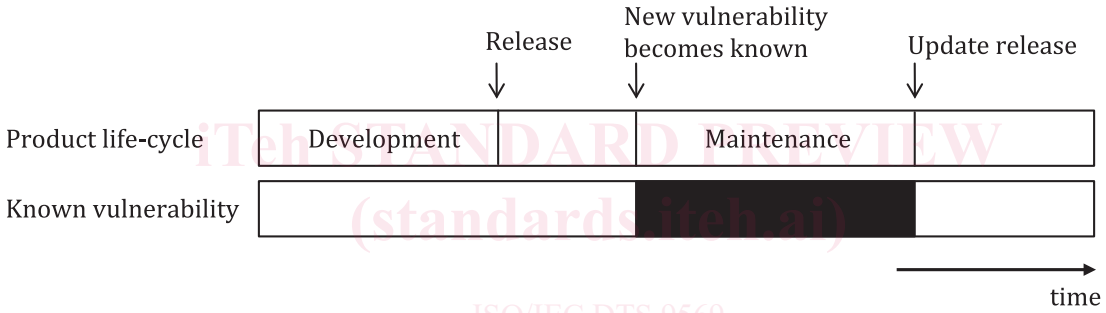
3.21
vulnerability
weakness in the *target of evaluation* (3.18) that can be used to violate the security functional requirements in a specified environment

Note 1 to entry: In the definition of ALC_PAM.1 in Clause 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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-

Key

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

Figure 1 — Product vulnerability timeline

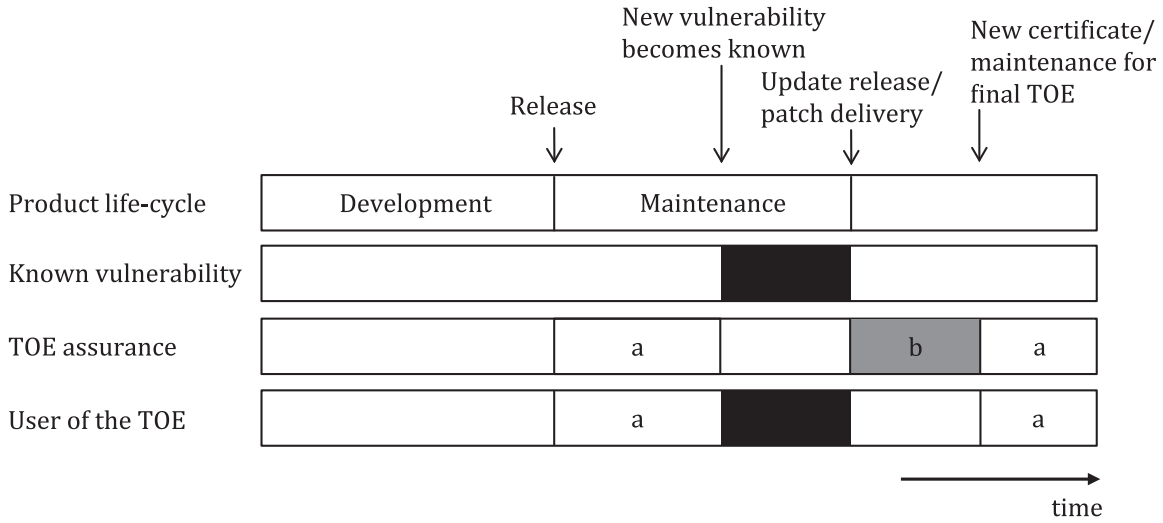
Consequently, developers have a responsibility to build and release those updates in a short period of time after the vulnerability becomes known. Developers who obtained a certificate previously may request a re-evaluation of the TOE (for example for issuing a new certificate, or because it is mandated 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



Key

■	The TOE is vulnerable due to the lack of a patch.
▭	The user is unable to decide whether it is better to use the evaluated TOE or the patched TOE.
a	The user can use the (re-)evaluated TOE.
b	Time for maintenance / re-certification.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 2 — Timeline showing availability of patch and the corresponding new certificate

ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-

The focus is on the time for maintenance or re-certification (see Figure 2), in particular:

— how to ease re-evaluations, to optimally shorten the time for maintenance or re-certification;

— how to give some degree of assurance to the user so that, during this maintenance or re-certification period, they can choose to deploy the patched TOE.

This proposed patch management extension has the following advantages for the different stakeholders:

— Easing the re-evaluation process, therefore helping regulatory bodies in mandating re-evaluations when needed.

— Helping users to resolve the dilemma of whether to keep the evaluated version, or move to the patched version, by providing some degree of assurance on the patched TOE by assessing, during the initial evaluation that:

  — the patch deployment process provides procedural security measures against the introduction of regressions;

  — the TOE security functionality, including mechanisms allowing the TOE to be patched, are evaluated for conformity and robustness to avoid introducing vulnerabilities on the TOE.

— Helping developers by providing a standard way to assess the security of their patch development and deployment processes, as well as standard requirements to define the patching capabilities of their products.

— Helping evaluation authorities with a set of options they can provide within their policies to the customers (i.e. developers) to offer flexible and modern evaluation approaches.

© ISO/IEC 2023 – All rights reserved

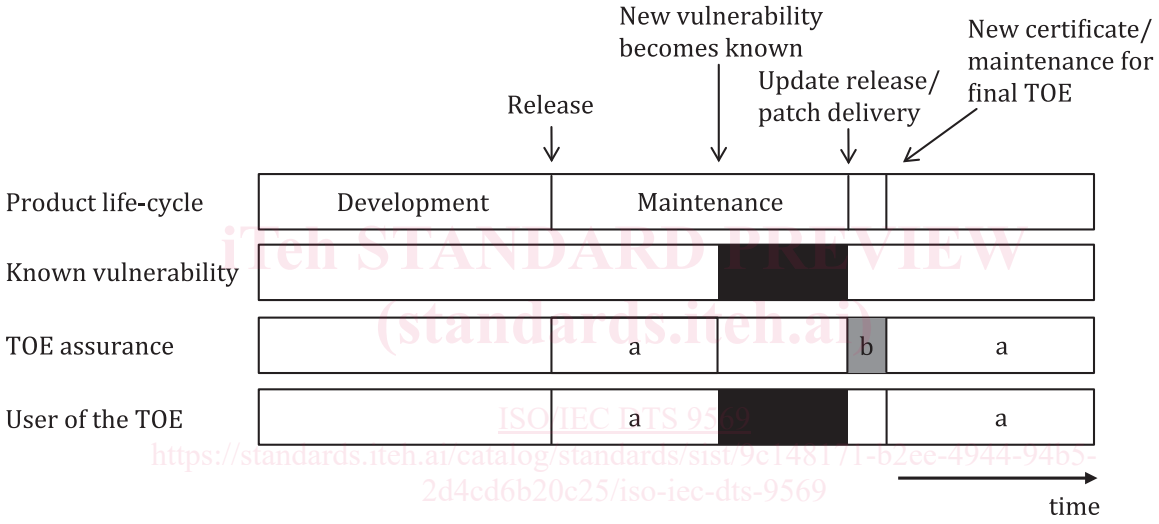
4.2 Proposed approach

The solution involves the following two aspects:

— Add additional functional requirements which address the patch or update functionality of the initial TOE. This document does not define mandatory content for the security problem definition or security functional requirements (SFRs). The security target or protection profile should contain TOE or TOE-type specific information. To facilitate the authoring of these documents, Annex C gives an example for a security problem definition and corresponding objectives. Additionally, Annex D includes guidance on how to write SFRs for the patch functionality.

— Add additional life cycle requirements (ALC_PAM) to get commitment from developers to consistently monitor for flaws or issues after release of the initial TOE, but also encourage developers to consistently generate evidence for future re-evaluations (see 5.2).

Figure 3 shows the application of ALC_PAM, which supports the timely delivery of the patch or update, but also the maintenance of the internal and external assurance activities.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9e148171-82ee-4944-9465-2d4cd6b20c25/iso-iec-dts-9569

Key

■	The TOE is vulnerable due to the lack of a patch.
■	The user is unable to decide whether it is better to use the evaluated TOE or the patched TOE.
a	The user can use the (re-)evaluated TOE.
b	Time for maintenance / re-certification.

Figure 3 — Timeline showing application of ALC_PAM

4.3 Non-public vulnerabilities

For many IT products, researchers discovering vulnerabilities are incentivised to not disclose the vulnerabilities until the developers have had an opportunity to patch them. In this case, it is plausible that the end user of the TOE is not aware of the vulnerability and the presence of the vulnerability can be considered a residual risk inherent to the use of any IT product. Consequently, many security patches are issued prior to end users and the public being made aware of the vulnerability.

The assurance family ALC_PAM introduced in this document provides a way to increase the assurance on developer patching procedures. When vulnerabilities are reliably fixed by patching procedures before the vulnerability is made public, there is less opportunity for successful attacks.

© ISO/IEC 2023 – All rights reserved

5 Patch management family

5.1 General

This clause defines the new assurance family ALC_PAM.

The security assurance requirements (SARs) introduced in 5.2 are related to different evaluation phases. During initial evaluation of the TOE, additional evaluation actions shall be introduced (compared to the standard SAR from ISO/IEC 15408-3) to establish assurance for the future patch generation process. The concept is to define ALC_PAM (patch management) and augment this family during initial evaluation in the security target.

As patch management is part of the life cycle assurance, it has been introduced under the ALC class. ALC_PAM describes how to handle patches life cycle, design, development, validation and release, but not the remediation flow. For this reason, ALC_PAM is not part of ALC_FLR (flaw remediation) even if a patch is a fix for a flaw managed in accordance with ALC_FLR. Both classes are closely related and therefore the dependency with ALC_FLR.2 was defined.

ALC_PAM, contrastingly, aims to support maintenance of the TOE assurance over the product life cycle. This family requires developers to provide a patch management policy and to follow this policy to develop patches for the TOE at the time of evaluation. This family also requires developers to define a procedure for the self-assessment to maintain the quality of the TOE after its evaluation. The developer can publish the result of the self-assessment to show the current status of the latest version of the TOE (e.g. re-evaluation is required or assurance is maintained) to the TOE users.

Annex B contains an example of a patch policy which fulfils the given requirements.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.2 Patch management (ALC_PAM)

5.2.1 Objectives

ISO/IEC DTS 9569
https://standards.iteh.ai/catalog/standards/sist/9c148171-b2ee-4944-94b5-

The objective of this family is to identify the policies and procedures to be implemented in the development process, which will be applied after the initial release of a TOE by the developer.

The application of the patch management (PAM) process cannot be always determined at the time of the initial evaluation. Nevertheless, it is possible to evaluate the policies and procedures that a developer has in place to perform the PAM process for a future patch release. It is also possible to obtain some evidence of the correct application of the procedures during the patching of the problems which are found during the evaluation of other assurance classes like AVA (vulnerability assessment) and ATE (tests).

The written PAM policies, processes and procedures are internal documents for the developer. These shall include instructions, among others, on how developers securely provide guarantees of authenticity to distribute and apply patches and how the life cycle of the keys, used for providing authenticity of new patches, is handled.

These procedures shall guarantee the secure development, the secure deployment, installation and activation for patches. Moreover, the procedures and the set of commands supporting them shall be described in the AGD (guidance) family.

5.2.2 Component levelling

This family contains only one component.

5.2.3 Application notes

None.

© ISO/IEC 2023 – All rights reserved