Assurance Package for Flaw Remediation

Version: 1.0

2024-06-28

National Information Assurance Partnership

Revision History

Version	Date	Comment
V1.0	2024-06-28	Initial draft

Table of Contents

1 Introduction

1.1 Package Identification

This assurance package is identified as follows:

- Name: Assurance Package for Flaw Remediation
- Version: 1.0
- Date: June 28, 2024
- Sponsor: National Information Assurance Partnership (NIAP)
- Applies to: CC version 3.1 revision 5 Part 3

1.2 Overview

Ongoing security maintenance is critical to protecting products against novel attacks, vulnerable dependencies, and security flaws that may be introduced through feature enhancements or other product changes. The Common Criteria (CC) defines ALC_FLR, Flaw Remediation, specifically to ensure that the developer of a certified product has procedures put into place to ensure that potential flaws are diagnosed and addressed. ALC_FLR includes three hierarchically increasing levels (ALC_FLR.1 through ALC_FLR.3) that define flaw remediation procedures to an increasing level of rigor.

This assurance package is intended to serve as an optional extension to Protection Profiles (PPs) and PP-Configurations for certifying schemes that require flaw remediation procedures when exact conformance is required. CC validation schemes may require a conformant product include any level of ALC_FLR in its validation process to obtain sufficient assurance that product security is maintained on an ongoing basis.

1.3 Terms

The following sections provide both CC and technology terms used in this assurance package.

1.3.1 Common Criteria Terms

Term	Meaning
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one PP and at least one PP-Module.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.

1.3.2 Technology Terms

No technology-specific terms are defined in this assurance package.

1.4 Compliant Targets of Evaluation

The Target of Evaluation (TOE) for this assurance package is any product that is certifiable under the CC that is capable of undergoing flaw remediation. Typically this will refer to products that claim a security functional requirement (SFR) related to trusted update, most commonly FPT_TUD_EXT.1. A PP or PP-Configuration that defines a conformant TOE as having immutable software or firmware is not expected to have a flaw remediation process beyond a full replacement of the product.

This package solely consists of the ALC_FLR family of Security Assurance Requirements (SARs) as defined in Part 3 of the CC. Each component in this family has no dependencies, so there are no requirements or restrictions for their inclusion; a conformant Security Target (ST) simply includes the assurance package in the set of claimed assurance requirements and claims one of the components. ALC_FLR requires evidence that adequate flaw remediation procedures for internal use are documented, and that flaw remediation guidance addressed to TOE users is provided; it does not require anything to be applied to the TOE itself that would affect how it is described in the ST.

Note that ALC_FLR is fully hierarchical; a claim of ALC_FLR.3 is automatically inclusive of both ALC_FLR.1 and ALC_FLR.2, and a claim of ALC_FLR.2 is automatically inclusive of ALC_FLR.1.

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this assurance package, as defined in the CC and CEM addenda for Exact Conformance, Selection-based SFRs, and Optional SFRs (dated May 2017).

CC Conformance Claims

This assurance package is conformant to CC Version 3.1, Revision 5 Part 3 (conformant). No Part 2 claim is made as assurance packages do not contain functional requirements.

PP Claims

This assurance package does not claim conformance to any Protection Profile.

Package Claims

This assurance package does not claim conformance to any packages.

3 Security Assurance Requirements

The following SARs are all optional requirements which may be included in the ST but are not required in order to conform to a PP or PP-Configuration which are conformant to this package.

3.1 ALC_FLR.1 Basic Flaw Remediation

3.1.1 Developer Action Elements

3.1.1.1 ALC_FLR.1.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

3.1.2 Content and Presentation Elements

3.1.2.1 ALC_FLR.1.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

3.1.2.2 ALC_FLR.1.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

3.1.2.3 ALC_FLR.1.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

3.1.2.4 ALC_FLR.1.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

3.1.3 Evaluator Action Elements

3.1.3.1 ALC_FLR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

3.2 ALC_FLR.2 Flaw Reporting Procedures

3.2.1 Developer Action Elements

3.2.1.1 ALC_FLR.2.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

3.2.1.2 ALC_FLR.2.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

3.2.1.3 ALC_FLR.2.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

3.2.2 Content and Presentation Elements

3.2.2.1 ALC_FLR.2.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

3.2.2.2 ALC_FLR.2.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

3.2.2.3 ALC_FLR.2.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

3.2.2.4 ALC_FLR.2.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

3.2.2.5 ALC_FLR.2.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

3.2.2.6 ALC_FLR.2.6C

The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

3.2.2.7 ALC_FLR.2.7C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

3.2.2.8 ALC_FLR.2.8C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

3.2.3 Evaluator Action Elements

3.2.3.1 ALC_FLR.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

3.3 ALC_FLR.3 Systematic Flaw Remediation

3.3.1 Developer Action Elements

3.3.1.1 ALC_FLR.3.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

3.3.1.2 ALC_FLR.3.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

3.3.1.3 ALC_FLR.3.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

3.3.2 Content and Presentation Elements

3.3.2.1 ALC_FLR.3.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

3.3.2.2 ALC_FLR.3.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

3.3.2.3 ALC_FLR.3.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

3.3.2.4 ALC_FLR.3.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

3.3.2.5 ALC_FLR.3.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

3.3.2.6 ALC_FLR.3.6C

The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

3.3.2.7 ALC_FLR.3.7C

The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

3.3.2.8 ALC_FLR.3.8C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

3.3.2.9 ALC_FLR.3.9C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

3.3.2.10 ALC_FLR.3.10C

The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

3.3.2.11 ALC_FLR.3.11C

The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

3.3.3 Evaluator Action Elements

3.3.3.1 ALC_FLR.3.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

4 Appendix A. Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017