APPLICATION NOTE

INTERPRETATION OF THE CC COMPONENT ANALYSING THE PROCEDURES FOR THE SYSTEMATIC CORRECTION OF SECURITY FLAWS (ALC_FLR.3)

Application   :   From publication

Circulation   :   Public

COURTESY TRANSLATION

Modifications

Version	Date	Modifications
1	15/10/08	Creation

TABLE OF CONTENTS

Purpose of the note

This note sets forth the interpretation as applied in the French scheme of the terminology found in assurance component ALC_FLR.3.

1. References

- [CC v2.3] : Critères Communs Parts 1-2-3 and CEM ; version 2.3 ; August 2005 ; ref. : CCMB-2005-08-001 to 004
- [CC v3.1] : Critères Communs Parts 1-2-3 and CEM ; version 3.1 ; June 2006 ; ref. : CCMB-2006-06-001 to 004

2. Interpretations

The following chapters provide, for each term requiring interpretation, a reminder of the requirements of the content as described in the Common Criteria (requirement "C"), as well as the work units associated with these requirements as described in the evaluation methodology.

2.1. « Corrected »

The [CC v2.3] and [CC v3.1] introduce the term "*corrected*" in the following criteria:

[CC v2.3]	[CC v3.1]	
ALC_FLR.3.6C		The procedures for processing reported security flaws shall ensure that any reported flaws are *corrected* and the correction issued to TOE users.
	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.
ALC_FLR.3-7	ALC_FLR.3-9	The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would help to ensure that every reported flaw is *corrected*.

Interpretation: "*correction*" or "*remediation*" should be understood as meaning "corrective measures".

These corrective measures do not necessarily consist in the issuing of patches for the product. They may be non-technical, e.g. they may correspond to the issuing of adapted configurations or user rules rendering the security flaw inoperative.

2.2. « Timely »

The [CC v2.3] and [CC v3.1] introduce the term "*timely*" in the following criteria:

[CC v2.3]	[CC v3.1]	
ALC_FLR.3.9C	**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.
ALC_FLR.3-11	**ALC_FLR.3-7**	The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in a *timely* means of providing the registered TOE users who might be affected with reports about, and associated corrections to, each security flaw.

Interpretation: "*Timely response*" in this context means "response within a limited time". The scheme does not impose any requirements on the developer concerning the time he/she takes to identify and circulate appropriate corrective measures.

On the other hand, the evaluation sponsor must define an acceptable response time, which must be communicated to the certifier and evaluator at the outset of the evaluation.

2.3. « Automatic distribution »

The [CC v2.3] and [CC v3.1] introduce the term "*automatic distribution*" in the following criteria:

[CC v2.3]	[CC v3.1]	
ALC_FLR.3.9C	**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.
ALC_FLR.3-12	**ALC_FLR.3-8**	The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in *automatic distribution* of the reports and associated corrections to the registered TOE users who might be affected.
ALC_FLR.3-12	No equivalent	The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in *automatic distribution* of the reports and associated corrections to the registered TOE users who might be affected

Interpretation: "*Automatic distribution*" should be understood as meaning "systematic distribution": these criteria enable to ensure that the distribution procedures are adequate in order to guarantee that all identified security flaws are effectively reported to users of the product concerned who may be affected by said flaw, and that the corrective measures are circulated to said users.