
I-0410: Auditing Of Subject Identity For Unsuccessful Logins

TYPE: NIAP Interpretation
 NUMBER: I-0410
 STATUS: Ready for External Review

 TITLE: Auditing Of Subject Identity For Unsuccessful Logins

 SOURCE REFERENCE: CC v2.1 Part 2 Subclause 3.2 FAU_GEN.1
 CC v2.1 Part 2 Subclause 3.2 FAU_GEN.2
 CC v2.1 Part 2 Subclause C.2 FAU_GEN.1
 CC v2.1 Part 2 Subclause C.2 FAU_GEN.2

 RELATED TO: <None>

ISSUE:

Both the FIA_UAU and FIA_UID components call for auditing of unsuccessful logins. However, if the login is unsuccessful, there is no subject identity to put in the audit record (as there is no subject in place). This is an inconsistency.

In a similar fashion, FAU_GEN.2.1 cannot be satisfied in the face of an invalid login, for there is no identity of the user that caused the event.

STATEMENT

For unsuccessful login attempts, it is acceptable to not include the subject identity in the login record.

SPECIFIC INTERPRETATION:

Note: The following presumes that I-0429 is approved before I-0410

To address this interpretation, the following changes are made to CC v2.1 Part 2: (additions marked thusly; deletions marked ~~thusly~~)

- FAU_GEN.1-NIAP-0429 is relabeled as FAU_GEN.1-NIAP-0410. Unless otherwise noted in these changes, all normative and informative material associated with FAU_GEN.1-NIAP-0429 is incorporated unchanged into FAU_GEN.1-NIAP-0410, and all references to FAU_GEN.1-NIAP-0429 in the CC, CEM, or other Common Criteria documentation is changed to refer to FAU_GEN.1-NIAP-0410.
- FAU_GEN.1.2 is replaced with the following:

FAU_GEN.1.2-~~NIAP-0407~~-NIAP-0410 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event time, based on the auditable event definitions of the functional components included in the PP/ST, [selection: [assignment: *other audit relevant information*], "*no other information*"]

- The following paragraph is added in Subclause C.2, after paragraph 565:

Note: It is not always possible to record the subject identity in an audit record. This can happen, for example, during an invalid login attempt, where there is no user subject involved. In such cases, it is acceptable to record that no user subject was involved.

- FAU_GEN.2 is relabeled as FAU_GEN.2-NIAP-0410. Unless otherwise noted in these changes, all normative and informative material associated with FAU_GEN.2 is incorporated unchanged into FAU_GEN.2-NIAP-0410, and all references to FAU_GEN.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FAU_GEN.2-NIAP-0410.
- FAU_GEN.2.1 is replaced with the following:

For audit events resulting from actions of identified users, ~~The~~ the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

- The following paragraph is added in Subclause C.2, after paragraph 572:

Note: FAU_GEN.2.1 is not applicable when there is no validated user identity to associate with the auditable action. This can occur, for example, when login is unsuccessful.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This queue entry is dependent on I-0429 and I-0407, and should not be approved before those entries.

At the time of an unsuccessful login, there is no user subject whose identity can be recorded. Similarly, there is no validated user identity to associate with that audit event. Thus, it is appropriate to not include such information in the audit record, or to record an indication that the indicated field is not applicable.