Record ID: VID10403-0008-ACMR

CCEVS Approved Assurance Continuity Maintenance Report

Product:	Cisco Unified Computing System (UCS)
EAL:	4 Augmented with ALC_FLR.2
Date of Activity:	28 February 2013
References:	Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008 Impact Analysis Report for Cisco Unified Computing System (UCS), Version 1.0, December 2012
Documentation Updated:	Cisco Unified Computing System (UCS) Security Target, Version 1.1, November 2012 Cisco Unified Computing System (UCS), version 2.0(4b) Common Criteria Operational Usere Guidance and Preparative Procedures, Version 1.1, December 2012

I. Introduction

In December 2012, Cisco submitted an Impact Analysis Report (IAR) for the Cisco Unified Computing System (UCS) to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the Cisco Unified Computing System (UCS), the evidence updated as a result of the changes and the security impact of the changes.

II. Changes to the TOE

1. Hardware Changes

- Models removed from the TOE:
  - 2248TP Fabric Extender
- Models added to the TOE:
  - Blade Servers:
    - B200 M3
    - B230 M2
    - B440 M2
    - B22 M3
    - B420 M3
  - Rack-Mount Servers:

        - C200 M2SFF
        - C220 M3
        - C240 M3
        - C260 M2
        - C460 M2
        - C22 M3
        - C24 M3
    - Fabric Interconnects:
        - 6248UP
        - 6296UP
    - Fabric Extenders:
        - 2204XP
        - 2208XP
        - 2232PP

2. **Software Changes**
    - Bug fixes. See detail in section 5.1 of the IAR report.

3. **Changes to Customer-Facing Documentation**
    - ST: Updated to reflect the updated software versions noted above.
    - AGD_PRE and OPE: Updated to reflect the updated software versions noted above.

III. Analysis and Testing

1. Summary of Change Analysis

Cisco UCS bug fixes are tracked within Cisco's defect tracking system (CDETS). Each bug, whether identified by a customer or within Cisco is tracked within CDETS, and given a CDETS identifier. Each CDETS bug report contains a brief "headline" and more detailed discussion of the problem and the resolution. The vendor examined each of the detailed CDETS reports and drafted the "brief description" found in the tables of the IAR by referencing the CDETS headline and the report details. The vendor made the determination of which category was applicable for each report by:

a. Examining the "headline" and immediately classifying those that involved items that were excluded from the TOE or had no security relevance (such as grammatical corrections to help files) into the "Minor Changes with Little or No Security Relevance" category. This ruled out more than half of the reports.

b. For the remaining items, the details of the report were examined, including what the implications of the noted issue was, and what changes were required. Fields such as the report summary, how the report was found, workarounds, and attachments that showed device captures, test results, and configurations applicable to the report were examined to determine security relevance. Once again, the vendor was able to classify a large number of reports into the "Minor Changes with Little or No Security Relevance" category as they were unrelated to the TSC. (See Section 5.2 under "Examples of minor bug fixes that are not related to the TSC" for specific groups of reports that were classified in this manner.)

c. The items that were found to be related to the TSC were noted as such and then the vendor examined them in detail to determine whether they involved a change that made the TSC behave as advertised or involved major changes that jeopardized the TSC enforcement. The vendor also determined which TOE Security Function was applicable for each of these reports.

Each of the fixes fall into the following categorizations:

- Minor Changes with Little or No Security Relevance: These changes may be related to the TSC in some way, though may or may not relate directly to an SFR defined within the ST.

- Minor Changes with Some Security Relevance: These changes relate to the TSC in some way though the affect of the change is only to ensure the TOE functions as expected, and does not add or detract from the stated requirements in the ST. Therefore, changes in this category result in no adverse affect to the assurance baseline.

None of the fixes fall into this category:

- Major Changes: These changes can be directly related to some SFR, and modify how the TOE meets that SFR such that the TSS or design documents are no longer accurate.

2. Summary of the Vendor's Analysis

2.1 Minor Changes with Little or No Security Relevance

2.1.1 Changes to Non-Executable Text in the Source Code

Table 6 of the IAR lists 10 updates to the syntax, spelling, and grammar used in a command that have no bearing on the security relevance of the command, or that restore the command to its functionality as described in the evaluation documentation and do not interfere with the TSF. Updates to the documentation (command references and configuration guides) have no effect on the TSF, as the updated guides are part of the new evaluation record. Updates to the help messages displayed for commands have no effect on the TSF. Updates to comments within the code have no effect on the TSF. All updates to the TOE that dealt with these scenarios were not applicable to the TSF.

2.1.2 Cosmetic Changes

Table 7 of the IAR lists 45 cosmetic changes impact usability or "user-friendliness" but do not impact security relevant functions of the TOE.

2.1.3 Incorrect, inconsistent, or missing information, irrelevant to the TSF

Table 8 of the IAR lists 19 bug fixes that were related to data viewable through administrative interfaces which were not entirely consistent or complete, but which are not relevant to the TSF.

2.1.4 Changes that are irrelevant to the TSF for various reasons

Table 9 of the IAR lists 2493 additional bug fixes that were determined to be irrelevant to the TSF for various reasons.

2.1.5 Performance, Scalability, and Stability Issues are Irrelevant to the TSF

Table 10 of the IAR lists 379 additional bug fixes that were determined to be related to performance, scalability and stability and thus irrelevant to the TSF.

2.2 Minor Changes with Some Security Relevance

2.2.1 Access Control and Roles

Table 11 of the IAR lists 5 bug fixes that were determined to be related to access control and roles which were deemed to be minor in nature.

2.2.2 Redundant to Other CDETS Entries

Table 12 of the IAR lists 6 bug fixes that were determined to be redundant to other CDETS entries and thus addressed elsewhere.

2.2.3 Audit Generation, Protection, and Review, and Timestamps

Table 13 of the IAR lists 13 bug fixes that were determined to be related to audit generation, protection, and review, and timestamps which were deemed to be minor in nature.

2.2.4 Identification and Authentication

Table 14 of the IAR lists 30 bug fixes that were determined to be related to identification and authentication which were deemed to be minor in nature.

2.2.5 Various SFRs - Incorrect, Inconsistent, or Missing Information

Table 15 of the IAR lists 75 bug fixes that were determined to be related to various other SFRs because of incorrect, inconsistent, or missing information and were deemed to be minor in nature.

2.2.6 Guidance Documentation and Vulnerabilities

Table 16 of the IAR lists 9 bug fixes that were determined to be related to guidance documentation and vulnerabilities that were deemed to be minor in nature.

2.2.7 Management Functions (query, modify, delete, etc.)

Table 17 of the IAR lists 109 bug fixes that were determined to be related to management functions (query, modify, delete, etc.) that were deemed to be minor in nature.

2.2.8 New Hardware

Table 18 of the IAR lists 399 bug fixes that were determined to be related to the new hardware and deemed to be minor in nature.

2.2.9 Protection of the TSF

Table 19 of the IAR lists 20 bug fixes that were determined to be related to the protection of the TSF and deemed to be minor in nature.

2.2.10 VLAN Traffic Flow Control

Table 20 of the IAR lists 78 bug fixes that were determined to be related to the VLAN traffic flow control and deemed to be minor in nature.

2.2.11 VSAN Traffic Flow Control

Table 21 of the IAR lists 15 bug fixes that were determined to be related to the VSAN traffic flow control and deemed to be minor in nature.

IV. Conclusion

This maintenance activity covers the assessment of the evaluation impact of the changes applied to Cisco Unified Computing System (UCS) evaluated on several versions of Cisco hardware.

While a tremendous number of bug fixes are addressed in this update it was determined that the overall impact of the changes is minor.

In the changes from UCS 1.4(1m) to 2.0(4b) minor bug fixes were applied. UCS is built from millions of lines of code, the bug fixes applied to the software affect only a small fraction of that source code. Each fix was applied to make the TOE function as originally intended, no additional security functionality was added, and no existing security functionality was removed.

Types of minor bug fixes that are not related to the TSC include:

- Changes to non-executable text.
- Cosmetic changes
- Resolving incorrect, inconsistent, or missing information, which is irrelevant to the TSF.
- Up/downgrading software, and firmware, which is outside the scope of the TSF.
- Performance, scalability, and stability issues.

Types of minor bug fixes that are related to the TSC include fixes related to:

- New supported hardware
- Incorrect, inconsistent, or missing data relevant to some aspect of the TSF
- Access control and roles
- Audit generation, protection, and review, and timestamps
- I&A, and remote administration
- Management functions (query, modify, delete, etc.)
- Protection of channels between TOE components and for remote administration.
- Traffic flow control for VLANs
- Traffic flow control for VSANs

Given the above number of bug fixes since the originally certified version, and the relevance of bug fixes to numerous SFRs, Cisco re-ran for this Assurance Maintenance effort the entire set of test cases from the original Common Criteria evaluation with satisfactory results.