Indian CC Certification Scheme (IC3S)

Certification Maintenance Report

Report Number : IC3S/KOL01/TEJAS/EAL2+/1020/0026/CR

Product / system : **TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively**

Dated: 22 Nov 2020

Version: 1.0

Government of India
Ministry of Electronics & Information Technology Standardization, Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road,
New Delhi –10003 India

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

"TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively"

1. **Maintenance Report Number**: IC3S/KOL01/TEJAS/EAL2+/1020/0026/CR

2. **Date**: **22 Nov 2020**

3. **References**:
    I. *D10 –Assurance Continuity Guidance for Maintenance and Re-evaluation of CC Certification under IC3S (STQC/CC/D10 Issue:03)*
    II. Impact Analysis Report of TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively, Version: 1.0
    III. IC3S/KOL01/TEJAS/EAL2/0316/0005

4. Description of changes

M/S Tejas Networks Limited submitted an Impact Analysis Report (IAR) for **"TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively"** to Indian Common Criteria Certification Scheme (IC3S) for approval on **22nd Oct 2020**. The IAR is intended to satisfy requirements outlined in "**D10-Assurance Continuity guidance for Maintenance and Re-evaluation of CC Certification under IC3S**". In accordance with those requirements, the IAR describes the changes made to the certified TOE/ TOE development environment, the evidence updated because of the changes, and the security impact of the changes.

5. Affected developer evidences

Developer Action Elements	Developer Documentation (change/inclusion)
ASE_INT.1	ST Introduction - ST reference -*(change)*
ASE_CCL	Conformance claims- *(change)*
ASE_REQ	Security requirements - the security assurance requirements (SARs)- *(change)*
ALC_DVS.1	i. ICT Policy, ver. 1.06 (*New*) ii. Tejas Policy & Security, V1.1(*New*) iii. *Procedure for Configuration Management,V1.04 (New)*

6. Result of Analysis of IAR

The developer of the TOE, M/S Tejas Networks Limited, has informed IC3S about a change in the development environment of the Certified Product, by including their "*Information communication and technology policy (ICT)*". The developer of the TOE claims that the ICT policy provides the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation, in its development environment. Hence, additional assurance measure ALC_DVS.1 is proposed for the Certified TOE. With this additional assurance measure, the developer requested to the CB for enhancement of Evaluation Assurance Level from **EAL2** to **EAL2+**.

From the submitted IAR the following observations are drawn:

i. The changes are in TOE development environment and not to the TOE.

ii.   The changes in the TOE environment has low impact to the Assurance Baseline i.e. from EAL 2 to EAL 2+

iii. Considering all above the, the impact of change is considered to be '**Minor'**. However, a subset evaluation and *partial* ETR is recommended before issue of a '**Maintenance Report'**.

iv.   As there is no change in the SFR, there is no need of additional effort in ATE class necessary for Assurance continuity from EAL2 to EAL2+.

v.   The product has been certified in Feb 2020, the developer has submitted IAR within one year of Certification and there is no publicly known change in the security threats perspective or attack method, related to this type of TOE; hence no additional   AVA_VAN activity is necessary to accommodate the request for change in the Certificate.

vi.   The following **subset evaluation** is recommended by the Scheme:
   a.   Evaluation of ST for ASE_INT.1, ASE_CCL and ASE_REQ
   b.   Evaluation of Life Cycle Support for ALC_DVS.1

7. Result of subset evaluation

The overall impact is minor. This is based on the above rationale that adoption of ICT policy by the developer have no impact on the security function of the certified TOE. However, this is intended to protect the confidentiality and integrity of the TOE design and implementation, in its development environment. The developer's claims on additional Assurance component ALC_DVS.1 have been examined by the same evaluation team who were involved in origination evaluation in Feb 2020 and found to be complied with the requirement of CC standard.

8. Conclusion

Considering the nature of the change and its impact on Security of the TOE the same is classified as minor. The objective evidences presented before the evaluation team indicate that the TOE development was carried out under requisite controlled environment which qualifies for ALC_DVS.1, however, this assurance claim (ALC_DVS.1) was absent during original certification due to absence of formal adaptation of ICT Policy by the developer.

The evaluation facility presented the results of **subset evaluation** and **partial ETR,** which conform to the CC requirement of successful evaluation of ALC-DVS.1**.** Based on the evaluation IAR and evaluation results, it is confirmed that the assurance baseline has been preserved, for those changes to the development environment**. Hence change in Assurance Level from EAL 2 to EAL2+ is accorded. An addendum to the original Certificate is issued and publicly listed.**

----------- 0 ---------