PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Maintenance Report DCSSI-2008/09-M01

Appliance MISTRAL TRC 7535 V4.6.2

Reference Certificate : DCSSI-2008/09

Courtesy Translation

Paris, 31 of July 2008

References

a) Assurance continuity procedure MAI/P/01.
b) Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+, référence : 61 485 069 – 805 révision L, Thales Communications
c) Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+ - version Lite, reference : 61 485 069 – 805 revision M, Thales Communications
d) Rapport de certification DCSSI-2008/09 - Boîtier MISTRAL TRC 7535 V4.6.1, 10 mars 2008, SGDN/DCSSI
e) Analyse d'impact sécurité/fonctionnel – Mistral v6.4.1 / v6.4.2

Identification of the maintained product

The maintained product is the appliance MISTRAL TRC 7535 V4.6.2 developed by Thales Communications.
The maintained version of the product can be identified by the following elements:

- The hardware appliance TRC 7535 version 4, including an specific electronic card with a serial and Ethernet interfaces, a card reader (CAM), and an interface for emergency deletion of critical assets,
- The VPN IP software version 4.6.2.1 embedded in the appliance,
- The software embedded in the cryptographic module (FPGA) AES v2.0,
- The software for remote administration (CGM) version 6.2.1 that communicates with a front-end appliance MISTRAL TRC 7535, allowing the protection of communication between the CGM and other Mistral appliances.

These elements can be checked by the users: the appliance is physically labelled with its type and reference of the embedded cryptographic module, and the CGM allows checking the version of the embedded software in any Mistral appliance.

Description of changes

The target of evaluation (TOE) has evolved as follow:

- The VPN IP software has changed through version 4.6.2.1: this change is realised in order to allow all Mistral appliance managed remotely to provide the address of their active CGM for the standard appliance, and the management of the virtual address for the front-end appliance. This change is performed in order to enable the redundancy functionality between sites.
- The CGM software has changed through version 6.2.1: this functionality is extended in version 2 to the CGM redundancy between several sites. The local CGM redundancy is also extended with the possibility to virtualize two couple of front-end appliance/CGM within the same site, through virtual address.
  The management center (CG) redundancy can be set with two mechanisms:
  - The use of two address for the management center;
  - The virtualization of the CG and front-end address.

  It is therefore possible to enable a CG redundancy with 4 CGM.

Impacted deliverables

The deliverables impacted are:

- Security target;
- Configuration list;
- User and administrator guidance;
- Source code of the software embedded.

[CONF]	CSCI Boîtier Mistral – Document de description de version (VDD), Reference: 61 484 104 AF - 498 Rev H
[GUIDES]	- TRC 7535 Mistral v4.6.1, Manuel utilisateur (SUM), Reference: 61 484 290 AF, 108 fr revision B, Thales Communications - Centre de Gestion Mistral, Manuel utilisateur (CGM_SUM), Reference: 46 250 239 05 – 108 revision G, Thales Communications
[ST]	Cible de sécurité Mistral (CDS) MISTRAL TRC735 EAL3+, reference: 61 485 069 – 805 revision M, Thales Communications

Conclusions

The above listed changes are considered as having a **minor** impact.
The assurance level of this new product revision is thus identical to the certified revision.

Warning

The resistance level of a certified product is declining as time goes by. The vulnerability analysis of this product revision versus the new attacks that would have appeared since the certificate release has not been conducted in the frame of this current maintenance. Only a re-evaluation or a "surveillance" of the new product revision would allow maintaining the assurance level in a timely and efficient manner.

Recognition of the certificate

European recognition (SOG-IS)

The reference certificate was issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

International common criteria recognition (CCRA)

The reference certificate was released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[1], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

This maintenance report is released in accordance with the document: « Assurance Continuity: CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

1 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.