Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de maintenance DCSSI-2008/09-M01

Boîtier MISTRAL TRC 7535 V4.6.2

Certificat de référence : DCSSI-2008/09

Paris, le 31 juillet 2008

Le Directeur central de la sécurité des systèmes d'information

Contre-amiral Michel Benedittini
directeur adjoint de la direction centrale
de la sécurité des systèmes d'information
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

a) Procédure MAI/P/01 Continuité de l'assurance
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, référence : 61 485 069 – 805 révision 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 du produit maintenu

Le produit maintenu est le boîtier MISTRAL TRC 7535 V4.6.2, développé par Thales Communications.
La version maintenue du produit est identifiable par les éléments suivants :

- le boîtier MISTRAL TRC 7535 version 4, incluant une carte électronique spécifique, et disposant d'une interface série, Ethernet, d'un lecteur de carte à microprocesseur (CAM), ainsi que d'une interface d'effacement d'urgence ;
- le logiciel VPN IP version 4.6.2.1 embarqué dans le boîtier ;
- le logiciel embarqué dans la ressource cryptographique (FPGA) AES v2.0 ;
- le logiciel CGM version 6.2.1 qui interagit avec un boîtier MISTRAL TRC 7535 frontal, permettant la protection des flux de gestion des autres boîtiers.

Ces éléments peuvent être vérifiés : le boîtier comporte une étiquette qui mentionne le type du boîtier ainsi que les références du module cryptographique embarqué, et le logiciel d'administration permet de vérifier la version du logiciel embarqué.

Description des évolutions

La cible de l'évaluation (TOE) a évolué comme suit :

- Le logiciel VPN IP a évolué en version 4.6.2.1 : cette évolution est réalisée pour demander aux équipements télégérés de remonter l'adresse de leur CGM actif pour les boîtiers nominaux, et la gestion des adresses virtuelles pour les boîtiers frontaux. Ceci, afin de mettre en place la redondance inter-site.
- Le logiciel CGM a évolué en version 6.2.1 : Cette fonctionnalité est étendue en version 2 à la redondance CGM distante (inter-site). On étend également la redondance CGM local par la possibilité de virtualiser deux couples de CGM/Frontal d'un même site au moyen d'adresses virtuelles.
  La redondance CG est possible au travers de 2 mécanismes :
  - l'utilisation de deux adresses de Centre de Gestion ;
  - la virtualisation des adresses des Centres de Gestion et frontaux.

  Il est ainsi possible de mettre en œuvre une redondance CG à 4 CGM.

Fournitures impactées

Les fournitures impactées sont les suivantes :

- cible de sécurité ;
- liste de configuration ;
- guide utilisateur et administrateur ;

- code source du logiciel embarqué.

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

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, à la date de certification.

Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Le certificat initial a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

[1] Les pays signataires de l'accord sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, la République de Corée, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.