PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de maintenance M-2005/06

Micro-circuit ATMEL AT90SC12836RCT rev. E

Certificat de référence : 2005/20

Paris, le 30 septembre 2005

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

Références

a) Procédure MAI/P/01 Continuité de l'assurance
b) AT90SC12836RCT Security Target Lite, Référence : TPG0084A_26Jul05, ATMEL,
c) Rapport de certification 2005/20 - Micro-circuit ATMEL AT90SC12836RCT rev. E, 9 août 2005,
d) Toolbox 3.X Security Impact Analysis, Revision 00.03.01.03 to 00.03.01.04, Référence : Toolbox_SIA_V1.1 (21 September 2005), ATMEL.

Identification du produit maintenu

Le produit maintenu est le micro-circuit AT90SC12836RCT (référence AT58819 révision E) développé par la société ATMEL Smart Card Ics, et certifié en révision E sous la référence 2005/20. Ce micro-circuit inclut une librairie logicielle cryptographique stockée en ROM : Toolbox 3.x en version 00.03.01.04.

Description des évolutions

Les changements consistent en une mise à jour de la librairie cryptographique qui est désormais en version 00.03.01.04. Ce changement intervient pour corriger un dysfonctionnement, relatif à la routine d'attente de fin de calcul du coprocesseur. Ce dysfonctionnement pouvait corrompre les résultats d'un calcul lors de leur lecture (données aléatoires).
Deux routines de la librairie cryptographique ont été modifiées :

- la routine d'attente de fin de calcul du coprocesseur ;
- la routine qui renvoie le numéro de version de la librairie cryptographique (mise à jour du numéro renvoyé).

Fournitures impactées

Seuls les documents relatifs à l'identification du produit ont changé :

[CONF]	Toolbox Configuration List, Library version 00.03.01.04, TPR00150DX-6 Sep 05
[ST]	AT90SC12836RCT Security Target Lite, Référence : TPG0084B_09Sep05

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.

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.