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-2008/43-M01

Carte à puce JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE

Certificat de référence : DCSSI-2008/43

Paris, le 6 juillet 2009

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

a) Procédure MAI/P/01 Continuité de l'assurance
b) Cible de sécurité : JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target - version 1.8 (la référence Développeur est CP-2006-RT-389)
c) Cible de sécurité publique : JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target Lite - version 1.4 (la référence Développeur est CP-2007-RT-075)
d) Rapport de certification DCSSI-2008/43 : Carte à puce JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE, 19 décembre 2008, SGDN/DCSSI
e) Rapport d'analyse d'impact : JCLX80jTOP20ID Patch v1.6 Impact Analysis Report, version 1.0, 9 février 2009 (la référence Développeur est CP-2009-RT-073)

Identification du produit maintenu

Le produit maintenu est la « carte à puce JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE, version IFXv#27_0.1, révision de code v1.4 » développée par Trusted Logic SA.

C'est une carte à puce bi-mode (contact/sans contact) comportant une plate-forme d'exécution d'applets Java Card conforme aux spécifications Java Card 2.2.1 et VISA GlobalPlatform 2.1.1 - configuration 2 standard, masquée sur le composant SLE66CLX800PE d'Infineon Technologies. Le patch v1.4 est chargé en EEPROM (*Electrically Erasable Programmable Read only Memory* – mémoire programmable en lecture seule et électriquement effaçable).

Description des évolutions

Toutes les modifications qui étaient déjà incluses dans le Patch File v1.4 sont également incluses, telles quelles, dans le Patch File v1.6, exceptée celle qui est décrite au chapitre §8.3 du [PV14]. Le code de cette modification a été optimisé afin de réduire la taille du Patch File en EEPROM. Cependant, le comportement fonctionnel de ce bout de code reste identique.

En plus des modifications existantes dans la version 1.4 du patch, le Patch File v1.6 corrige également les problèmes fonctionnels, listés ci-après, qui ont été identifiés par les utilisateurs :

- la carte se met en mutisme durant le traitement de certains APDU étendus. La correction du code concernant ce point est détaillée au chapitre §2.10 du [PV16] ;
- la commande READ BINARY utilisée par TL ICAO LDS et traitée par LDS FS API peut renvoyer 2 ou 3 octets de plus que la taille de la réponse spécifiée dans l'octet dit Le. Ceci est décrit au chapitre §5.7 du [PV16] ;
- la commande READ BINARY peut renvoyer une erreur lorsque l'offset spécifié dans la commande est égale à la taille du fichier. Ceci est décrit au chapitre §5.8 du [PV16].

Fournitures impactées

[ADV_LLD]	JCLX80jTOP20ID – Patch Description, Trusted Logic report CP-2007-RT-579, version 1.2 (edition for jTOP v27.01 – Patch File v1.4)
[ADV_IMP]	Tarball containing the sources of Patch File v1.4 deliverable reference ALCAZAR_V100_DELIVERY_SERMA_SOURCES_PATCH_V1_4_20080915
[PV14]	JCLX80jTOP20ID – Patch Description, Trusted Logic report CP-

	2007-RT-579, version 1.2 (edition for jTOP v27.01 – Patch File v1.4)
[PV16]	JCLX80jTOP20ID – Patch Description, Trusted Logic report CP-2007-RT-579, version 1.3 (edition for jTOP v27.01 – Patch File v1.6)

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 réévaluation 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 :

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[2], 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 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.
[2] 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, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.