PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance ANSSI-CC-2018/35-M01

Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h

OS Multos V4.5.2, AMD version 0151v001, Build number v1.1.47

Certificat de référence : ANSSI-CC-2018/35

Paris, le 18 décembre 2020

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

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 cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

1 Références

[CER]	Rapport de certification ANSSI-CC-2018/35, Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS Multos V4.5.2 et AMD version 0151v001, 30 août 2018.
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IC]	*BSI-DSZ-CC-1110-v2-2019 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h H13 including the products from the second production lune and optional software packages : Flash Loader, Asymmetric Crypto Library, Symmetric Cryptographic Library, Hardware Support Layer, Hash Crypto Library, Mifare Compatible Software, and CIPURSE Crypto Library,* 18 juin 2019.
[IAR]	*Impact Analysis Report – IDMotion V2 MULTOS Platform*, référence D1502303, version 1.3, 5 décembre 2019. *MULTOS P21, Security Impact Analysis buil*d, 1.1.42 vs 1.1.47, référence MI-SP-0653, version 1.0, 28 novemvre 2019.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.*
[CCRA]	*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.*

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS Multos V4.5.2, AMD version 0151v001, Build number v1.1.47 » développé par la société GEMALTO devenue aujourd'hui THALES.

Le produit « Plateforme IDMotion V2 masquée sur le composant IFX_CCI_000014h, OS Multos V4.5.2, AMD version 0151v001 » a été initialement certifié sous la référence ANSSI-CC-2018/35 (référence [CER]).

La version maintenue du produit est identifiable par les éléments suivants :

Configuration de la TOE	Données	Origine
OS version Multos	V4.5.2	THALES
Version du code correctif (AMD) IDMotion V2	v0151v001	
Build number	1.1.47	
Identifiant de la plateforme	0x16	
Donnée d'identification du circuit intégré	IFX_CCI_000014	INFINEON TECHNOLOGIES AG
Identifiant du *Firewall* de circuit intégré	80.100.17.3	

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- la prise en compte de mise à jour fonctionnelle du composant IFX_CCI_000014h (référence [IC]) ;
- les corrections des *bugs* fonctionnels suivants du logiciel embarqué :
  - la mauvaise manipulation des données d'entrée ALU lors de la vérification de signature en mode « *enhanced crypto* » qui pouvait entrainer un calcul sur de mauvaises valeurs ;
  - la gestion des interruptions WTX dans la fonction *hwStopWwtBwtTimer()* pouvant entrer dans une boucle infinie ;
  - une conversion de type dans la fonction *hwEraseDataItemStack()* pouvant impliquer un *mute* de la carte dans certaines configurations du produit ;
  - la correction sur la fonction de copie en RAM permettant la copie de données de 3 à 4 octets de longueur lorsque les adresses de la source et de la destination se chevauchent ;
  - la possibilité d'exécution d'une application jusqu'après la personnalisation sans *reset* préalable ;
  - l'enregistrement de *logs* pendant l'effacement de page mémoire lorsqu'un *tearing* est effectué ;
  - la possibilité de lancer une image *dual interface* sur un produit avec une interface contact afin d'améliorer la production des cartes ;
  - l'ajout d'une taille limite à la *data item stack* utilisée en phase de personnalisation ;
  - la prise en compte de toutes les données de sortie de la primitive *Get Random Number ;*
  - une correction de type en mode MULTOS Initialisation permettant de supporter les *extended APDU* ;
- les améliorations fonctionnelles suivantes du logiciel embarqué :
  - la modification de la constante OPTION_ROTATION_AREA_SIZE permettant une optimisation de la taille mémoire NVM ;
  - l'amélioration du temps de chargement pre-perso/codelet ;
  - l'ajout de la possibilité d'identifier les pré-chargement AMD avant l'activation ;
  - le retrait de la contrainte d'ordre du chargement d'application.

4 Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	*Multos Enablement*, référence MAO-DOC-TEC-101, version 1.2.	[CER]
	Multos GALU, Guide to Generating Application Load Units, référence MAO-DOC-TEC-009, version 2.9.	[CER]
	*Multos GLDA, Guide to Loading and Deleti*ng, reference MAO-DOC-TEC-008, version 2.28.	[CER]
	Multos MDRM, Multos Developer's Reference Manual, référence MAO-DOC-TEC-006, version 1.54.	[CER]
	Card Initialization Specification Multos ID Motion V2, référence D1459742, version 2.4.	[R-M01]

	Security Guidance for MULTOS Application Developers, référence MI-MA-0031, version 1.6.	[CER]
	Mask Verification Procedure, référence MI-PR-0012, version 1.1.	[CER]
[ST]	Cible de sécurité de référence : - *IDMotion V2 Platform Security Target*, référence ST_D1172991, version 1.97, 23 juin 2020 ; Version publique : - *IDMotion V2 Platform Security target*, référence ST_D1172991_P, version 1.5.	[R-M01]
[CONF]	Liste de configuration du produit : - LIS_IDMotionV2_LABEL_ceryneia.CCdoc-Maintenance-delivery_001, v1.1, 25 juin 2020 ; - LIS_cceryneia.CC-delivery_004 / 004, 28 février 2018 ; - LIS_cceryneia.Ccdoc-Labo-delivery_001 / 001, 28 juin 2018.	[R-M01]

5 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.

6 Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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 EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.