PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de surveillance ANSSI-CC-2018/02-S01

Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox v.06.04.01.07 et la bibliothèque Wear Levelling v.06.03.02.02

Certificat de référence : ANSSI-CC-2018/02

Paris, le 6 avril 2020

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

Guillaume POUPARD
[ORIGINAL SIGNE]

Avertissement

La surveillance du produit ne constitue pas en soi une recommandation d'utilisation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit soit totalement exempt de vulnérabilités exploitables.

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 technique d'évaluation : - Evaluation Technical Report (full ETR) – MISTRAL-E, référence LETI.CESTI.MISE.FULL.001 - V1.1, version 1.1 du 20/12/2017, *LETI*. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Report (ETR for composition) – MISTRAL-E, référence LETI.CESTI.MISE.COMPO.001 - V1.1, version 1.1 du 20/12/2017, *LETI*.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[RS-Lab]	Rapport technique de surveillance : - Evaluation Technical Report (full ETR) – MISTRAL-E, référence LETI.CESTI.MISE.FULL.001 – V2.0, version 2.0 du 16/3/2020, *LETI*
[ETR_COMP]	Evaluation Technical Report (ETR for composition) - MISTRAL-E, référence LETI.CESTI.MISE.COMPO.001 - V2.0, version 2.0 du 16/3/2020, *LETI*.

2. Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation *LETI*, permet d'attester que le produit « Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox v.06.04.01.07 et la bibliothèque Wear Levelling v.06.03.02.02 », certifié sous la référence [CER] peut être considéré comme résistant à des attaques de niveau AVA_VAN.5 dans les mêmes conditions et restrictions d'usage que celles définies dans [CER], lorsque les guides applicables [GUIDES] sont scrupuleusement respectés.

Il est à noter que de nouvelles recommandations sécuritaires ont été ajoutées au titre de la présente surveillance. Si ces recommandations ne sont pas mises en œuvre, le produit ne peut être considéré comme résistant à des attaques de niveau AVA_VAN.5.

Le rapport d'évaluation pour composition [ETR_COMP] a été mis à jour pour refléter les résultats de cette dernière surveillance.

La périodicité de la surveillance de ce produit n'est pas définie.

3. Guides applicables

Le tableau ci-dessous liste les guides applicables du produit évalué. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du guide correspondant.

Les guides contenant de nouvelles recommandations sécuritaires par rapport au certificat initial apparaissent en gras.

[GUIDES]	MS6xxx Technical Datasheet, référence TPR0702DX, version D du 9/3/2017, *WISEKEY*.	[CER]
	MS6001 Technical Datasheet, référence TPR0705EX, version E du 9/3/2017, *WISEKEY*.	[CER]
	Security Recommendations for MS6XXX 90nm Products – Application note, référence TPR706DX, version D du 10/3/2020, *WISEKEY*.	**[R-S01]**
	Security Hardware DES/TDES on MSXXX 90nm Products – Application note, référence TPR0707EX, version E du 10/1/2020, *WISEKEY*.	**[R-S01]**
	Security Hardware AES on MSXXX Products (90nm) – Application note, référence TPR0708DX, version D du 29/8/2017, *WISEKEY*.	[CER]
	Ad-X3 Datasheet, référence TPR0701CX, version C du 13/3/2017, *WISEKEY*.	[CER]
	Generating Random Numbers on MS6XXX Products (90nm) – Application note, référence TPR0709DX, version E du 6/3/2020, *WISEKEY*.	**[R-S01]**
	Toolbox 06.04.01.xx on MS6XXX – Application note, référence TPR0711HX, version H du 16/3/2017, *WISEKEY*.	[CER]
	TBX 06.04.01.XX Erratasheet – Application note, référence TPR0727DX, version D du 14/3/2017, *WISEKEY*.	[CER]
	Securing TBX 06.04.01.XX on MSXXXX 90Nm Products – Application note, référence TPR0712LX, version L du 10/3/2020, *WISEKEY*.	**[R-S01]**
	Wear Levelling library and low level FLASH drivers – Application note, référence TPR0710BX, version B du 5/1/2017, *WISEKEY*.	[CER]
	Efficient Use of Ad-X3 – Application note, référence TPR0726DX, version D du 14/3/2017, *WISEKEY*.	[CER]
	MS6XXX Secure Acceptance Guidance, référence TPR0754CX, version C du 28/1/2020, *WISEKEY*.	**[R-S01]**
	SmartACT's User Manual – Application note, référence TPR0134FX, version F du 18/8/2017, *WISEKEY*.	[CER]
	SC300 Technical Reference Manual, référence DDI0447A, version A du 29/6/2009, *WISEKEY*.	[CER]
	MS600X Customer Options Form, référence MS600X_COF_V1.1_RV, version 1.1 d'avril 2017, *WISEKEY*.	[CER]