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-2014/46-S05

Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révision 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE DESFire EV1 révision 3.7 ou 3.8

Certificat de référence : ANSSI-CC-2014/46

Paris, le 18 octobre 2019

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]	Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révision 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE DESFire EV1 révision 3.7 ou 3.8, 21 juillet 2014, ANSSI-CC-2014/46.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2014/46-S01 du 20 octobre 2015.
[R-S02]	Rapport de surveillance ANSSI-CC-2014/46-S02 du 9 décembre 2016.
[R-S03]	Rapport de surveillance ANSSI-CC-2014/46-S03 du 7 décembre 2017.
[R-S04]	Rapport de surveillance ANSSI-CC-2014/46-S04 du 12 décembre 2018.
[MAI]	Procédure ANSSI MAI/P/01 – Maintien de la confiance : Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2014/46-M01 du 17 mars 2016.
[R-M02]	Rapport de maintenance ANSSI-CC-2014/46-M02 du 18 janvier 2018.
[RS-Lab]	Evaluation Technical Report, Project : ANSSI-CC_2014/46, référence LAT_Surv2019_ETR, révision 3.0 du 8 octobre 2019, *THALES*.
[ETR_COMP]	Pour le besoin des évaluations ou surveillances en composition avec ce produit le rapport technique pour la composition a été mis à jour : Evaluation Technical Report for composite evaluation, Project : ST33G1M2 and derivatives, LATOUR Surveillance 2019, référence LAT_Surv2019_ETRLite, révision 1.0 du 8 octobre 2019, *THALES*.

2. Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation *THALES*, permet d'attester que le produit « Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révision 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE DESFire EV1 révision 3.7 ou 3.8 », 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], complétées par les recommandations sécuritaires additionnelles intégrées au fil des surveillances successives dans [GUIDES].

Ce résultat est applicable au produit « Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et 4.1.1 et la bibliothèque MIFARE DESFire EV1 révision 3.7 ou 3.8 » maintenu sous les références [R-M01] et [R-M02].

Il est à noter que de nouvelles recommandations sécuritaires ont été ajoutées au titre de la présente surveillance :

- si les recommandations incluses dans [SEC] ne sont pas mises en œuvre, le produit ne peut être considéré comme résistant qu'à des attaques de niveau AVA_VAN.4 ;
- **de plus, dès lors que la librairie cryptographique optionnelle NesLib v4.1 ou v4.1.1 est utilisée, si les recommandations de [SEC_NL] ne sont pas mises en œuvre le produit présente des vulnérabilités exploitables avec un potentiel d'attaque '*basic*' et ne peut satisfaire aucun composant d'assurance AVA_VAN.**

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 est de 1 an.

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. En particulier, [R-S05] référence la présente surveillance.

Les guides contenant de nouvelles recommandations sécuritaires par rapport à la précédente surveillance apparaissent en gras.

[GUIDES]	ST33G Platform – ST33G1M2 ST33I1M2: Secure MCU with 32-bit ARM SecurCore SC300 CPU and high density Flash memory – Datasheet, référence: DS_ST33G_I, révision 2, février 2017.	[R-S04]
	ST33G1M2 family extension – Technical note, référence TN_ST33G1M2_03, révision 1, juillet 2015.	[R-M01]
	ST33 uniform timing application note, référence AN_33_UT, révision 2, novembre 2013.	[CER]
	ST33G1M2 Firmware User Manual, référence UM_ST33G1M2_FW, révision 14, février 2019.	[R-S05]
	[SEC] ST33G and ST33H Security Guidance, reference AN_SECU_ST33, révision 8, mai 2019.	**[R-S05]**
	NesLib 4.1 and 4.1.1 for ST33 Secure MCUs cryptographic library User manual, référence UM_33_NESLIB_4, révision 4, décembre 2014.	[R-S02]
	[SEC_NL] ST33 Secure MCU family NesLib 4.1 security recommendations, référence AN_SECU_33_NESLIB_4, révision 10, septembre 2019.	**[R-S05]**
	ST33G and ST33H - AIS31 Compliant Random Number user manual, référence UM_33G_33H_AIS31, révision 3, octobre 2015.	[R-S05]
	ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, référence AN_33G_33H_AIS31, révision 1, octobre 2013.	[CER]
	MIFARE DESFire EV1 Library 3.7 for ST33G1M2 Secure MCUs – User Manual, référence UM_MIFARE_DESFire-EV1-3.7, révision 2, février 2013.	[CER]
	MIFARE DESFire EV1 Library 3.8 for ST33G1M2 Secure MCUs – User Manual, référence UM_MIFARE_DESFire-EV1-3.8, révision 1, avril 2013.	[CER]
	ST33G1M2 and derivatives – Flash loader installation guide, référence UM_33G_FL_v4, révision 4, août 2015.	[R-M01]