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-2017/73-S01

Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7

Certificat de référence : ANSSI-CC-2017/73

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 ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7, ANSSI-CC-2017/73, 18/12/2017.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[RS-Lab]	Evaluation Technical Report, Project : LATOUR AM2 Surveillance 2018, référence LATAM2_Surv2018_ETR, révision 3.0 du 08/10/2019, *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 ST33G1M2A1, LATOUR AM2 Surveillance 2018, référence LATAM2_Surv2018_ETRLite, révision 1.0 du 15/10/2019, *THALES*.

2. Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation *THALES*, permet d'attester que le produit « Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7 », 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].

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 v6.0.3 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-S0y+1] référence la présente surveillance.

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

[GUIDES]	Datasheet : ST33G1M2A - Automotive-grade secure MCU with 32-bit ARM SecurCore SC300 CPU and high-density Flash memory, référence DS_ST33G1M2A, révision 3.0, mai 2018	[R-S01]
	[SEC] Application note : ST33G and ST33h Secure MCU platforms Security guidance, référence AN_SECU_ST33, révision 8.0, mai 2019	**[R-S01]**
	Application note : ST33G and ST33H – AIS Reference importation : Start-up, on-line and total failure tests, référence AN_33G_33H_AIS31, révision 1.0, octobre 2013	[CER]
	User manual : ST33G and ST33H – AIS31 Compliant Random Number, référence UM_33G_33H_AIS31, version 3.0, octobre 2015	[CER]
	Cortex-M3 SC300 revision r0p0 Technical Reference Manuel », référence ARM_DDI_0037, révision F	[CER]
	User manual : ST33G1m2A/ST33G1M2M firmware, référence UM_ST33G1M2A_M_FW, révision 11.0, février 2019	[R-S01]
	User manual : Flash memory loader installation guide for the ST33G1m2A and ST33G1M2M platforms, référence UM_33GA_FL, révision 3.0, août 2016	[CER]
	User manual : NesLib cryptographic library NesLib 6.0, référence UM_NESLIB_6.0, révision 2.0, mars 2017	[R-S01]
	[SEC_NL] Application note : ST33 Secure MCU platforms NesLib 6.0 security recommandations, référence AN_SECU_ST33_NESLIB_6.0, révision 3.0, septembre 2019	**[R-S01]**
	Application note : StoreKeeper library 1.0 Security recommandations, référence AN_SECU_StoreKeeper, révision 1.0, janvier 2017	[CER]
	User manual : StoreKeeper v1.0, référence UM_StoreKeeper, révision 3.0, novembre 2016	[CER]
	User manual : Blackbox project – Developeur Kit system overview, référence OPE_UG_09_001, révision 2.02, août 2013	[CER]
	Datasheet : BlackBox – ST BlackBox interface, référence DS_BLACKBOX, révision 2, octobre 2012	[CER]
	Release note, NesLib 6.0.3 for ST33 platforms, référence RN_ST33_NESLIB_6.0.3, révision 4, juillet 2019	[R-S01]