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-2015/36-S02

Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1

Certificat de référence : ANSSI-CC-2015/36

Paris, le 30 avril 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

1. Références

[CER]	Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1, 15 septembre 2015, ANSSI-CC-2015/36.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2015/36-S01, 21 décembre 2016.
[MAI]	procédure ANSSI MAI/P/01 – maintien de la confiance : Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-20015/36-M01, 17 mars 2016.
[RS-Lab]	Evaluation Technical Report Project ST33H768, version 2.0, 20 avril 2018, LAT2_ETR, *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 Project ST33H768, version 2.0, 20 avril 2018, LAT2_ETRLite_1, *THALES.*

2. Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation *THALES*, permet d'attester que le produit « Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1 », 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 respectés.

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

Ce résultat est applicable au produit « Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4 et 5, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1 » maintenu sous la référence [R-M01].

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

[GUIDES]	ST33H Platform - ST33H768: Secure MCU with 32-bit ARM SecurCore SC300 CPU - and high density Flash memory – Datasheet, reference: DS_ST33H768, revision 4, April 2015.	[CER]
	ST33 uniform timing application note, reference: AN_33_UT, revision 2, November 2013.	[CER]
	ST33H768 Firmware User Manual, reference UM_ST33H768_FW, revision 5, May 2015.	[R-M01]
	ST33G and ST33H Security Guidance, reference: AN_SECU_ST33, revision 5.0, February 2016.	[R-S01]
	ST33G and ST33H - AIS31 Compliant Random Number user manual, reference UM_33G_33H_AIS31, revision 2, February 2014.	[CER]
	ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, reference AN_33G_33H_AIS31, revision 1, October 2013.	[CER]
	ST33 NesLib Library User manual, NesLib 4.1 and 4.1.1 for ST33 Secure MCUs, reference UM_33_NESLIB_4, revision 4, December 2014.	[CER]
	ST33 Secure MCU family NesLib 4.1 and NesLib 4.1.1 security recommendations, reference AN_SECU_33_NESLIB_4, revision 7, April 2015.	[CER]
	ST33H and derivatives – Flash loader installation guide, reference UM_33H_FL_v4, revision 4, August 2015.	[R-M01]

4. 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