Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2017/60-S02

ST31H320 B05

Certificat de référence : ANSSI-CC-2017/60

Paris, le 8 octobre 2019

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 de certification ANSSI-CC-2017/60, ST31H320 B01 including optional cryptographic library NESLIB, 5 octobre 2017.
[SUR]	Procédure ANSSI-CC-SUR-P-01 – Surveillance des produits certifiés.
[R-S01]	Rapport de surveillance ANSSI-CC-2017/60-S01, 28 août 2018.
[MAI]	Procédure ANSSI MAI/P/01 – Maintien de la confiance : Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2017/60-M01, ST31H320 B02 including optional cryptographic library NESLIB, 6 juillet 2018.
[RS-Lab]	Surveillance Technical Report S02 for LOUPIAC2 Project, LOUPIAC-2_S02_STR_v1.0 / 1.0, 26 septembre 2019, Serma Safety & Security.
[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 : Surveillance Technical Report Lite for Composition - S02 for LOUPIAC2 Project, LOUPIAC-2_S02_STR_Lite_v1.0 / 1.0, 26 septembre 2019, Serma Safety & Security.

2. Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation *SERMA SAFETY & SECURITY*, permet d'attester que le produit « ST31H320 B05 », 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 maintenu sous la référence [R-M01].

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 présente des vulnérabilités exploitables avec un potentiel d'attaque '*basic*' et ne peut satisfaire aucun niveau 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 version 'B05' du produit correspond notamment à cette liste.
La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du guide correspondant.

En particulier, [R-S02] référence la présente surveillance.

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

[GUIDES]	ST31H platform ST31H320, Datasheet – production data, DS_ST31H320 Rev 2, janvier 2016	[CER]
	ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, septembre 2010	[CER]
	ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, septembre 2010	[CER]
	ST31 firmware V3, User manual, UM_ST31G_H_FWv3 Rev 9, mars 2019	[R-S02]
	NesLib 4.2 library, User manual, UM_NESLIB_4.2 Rev 1.0, juillet 2015	[CER]
	ST31G and ST31H Secure MCU platforms NesLib 4.2 security recommendations, Application note, AN_SECU_ST31_NESLIB_4.2 Rev6, septembre 2019	**[R-S02]**
	NesLib 4.2.10 for ST31 platforms, release note, RN_ST31_NESLIB_4.2.10 Rev 9, août 2019	[R-S02]
	NesLib cryptographic library NesLib 5.2, User manual, UM_NesLib_5.2 Rev3, février 2019	[R-S02]
	ST31G and ST31H Secure MCU platforms NesLib 5.2 security recommendations, Application Note, AN_SECU_ST31_NESLIB_5.2 Rev 8, septembre 2019	**[R-S02]**
	NesLib 5.2.0 for ST31 platforms, Release note, RN_ST31_NESLIB_5.2.0 Rev 8, août 2019	[R-S02]
	ST31G and ST31H Secure MCU platforms, Security guidance, AN_SECU_ST31G_H Rev 6, avril 2019	**[R-S02]**
	ST31G and ST31H - AIS31 Compliant Random Number - User Manual, UM_31G_31H_AIS31 Rev 1.0, janvier 2015	[CER]
	ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, AN_31G_31H_AIS31 Rev 1, janvier 2015	[CER]