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 maintenance
ANSSI-CSPN-2019/03-M01

Ledger Nano S
Version 1.5.5 (2c970001)

Certificat de référence : ANSSI-CSPN-2019/03

Paris, le 7 août 2019

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

Emmanuel GERMAIN
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CSPN-2019/03 Ledger Nano S Version 1.5.1 (2c970001), 14 février 2019, ANSSI.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Security Impact Analysis from Ledger Nano S v1.5.1 to v1.5.5 Report, Release 1.0, 13 mars 2019, *LEDGER*.

2. Identification du produit maintenu

Le produit « Ledger Nano S, version 1.5.1 (2c970001) » a été initialement certifié sous la référence ANSSI-CSPN -2019/03 (référence [CER]).

Le produit objet de la présente maintenance est « Ledger Nano S, version 1.5.5 » développé par la société *LEDGER*.

La version maintenue du produit est identifiable, après authentification de l'utilisateur, en sélectionnant le menu *Settings*, puis *Device* et enfin *Firmware* qui expose la version 1.5.5 du *firmware* du SE.

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne les modifications suivantes :

- l'ajout du schéma de signature Shnorr afin d'être compatible avec *ZILLIQA* ;
- la modification de l'implémentation de Blake2 pouvant générer des sorties de taille autres que 224, 256, 384 ou 512 bits ;
- l'amélioration de l'expérience utilisateur ;
- la correction de bugs fonctionnels ;
- l'optimisation de la taille du code de la libraire cryptographique.

4. Conclusions

Les évolutions listées ci-dessus, qui interviennent sur des fonctionnalités hors TOE, sont considérées comme ayant un impact mineur sur la TOE précédemment évaluée.
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, dans les conditions du rapport [CER].

5. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

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