PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de surveillance ANSSI-CC-2017/81-S01

eTravel v2.2 on MultiApp v4.0.1 platform, BAC and AA activated

Annule et remplace le rapport de surveillance ANSSI-CC-2017/81-S01 du 16 septembre 2020

Certificat de référence : ANSSI-CC-2017/81

Paris, le 17 décembre 2021

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.

Le présent rapport annule et remplace le rapport de surveillance ANSSI-CC-2017/81-S01 signé le 16 septembre 2020 (correction effectuée au chapitre 2).

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-2017/81, eTravel v2.2 on MultiApp v4.0.1 platform, BAC and AA activated, 10 janvier 2018.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[RS-Lab]	S01 – Surveillance Technical Report – CASSIDY-E project, référence CASSIDY-E_STR_v1.1/ 1.1, version 1.1 du 11/6/2020, SERMA SAFETY & SECURITY.

Note : Le produit objet de la présente surveillance a été initialement développé par la société GEMALTO devenue aujourd'hui THALES DIS.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation SERMA SAFETY & SECURITY, permet d'attester que le produit « eTravel v2.2 on MultiApp v4.0.1 platform, BAC and AA activated », certifié sous la référence [CER] peut être considéré comme résistant à des attaques de niveau AVA_VAN.3 dans les mêmes conditions et restrictions d'usage que celles définies dans [CER], lorsque les guides applicables [GUIDES] sont strictement respectés.

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 composant d'assurance AVA_VAN.

La périodicité de la surveillance de ce produit est de 3 ans.

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-S01] référence la présente surveillance.

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

[GUIDES]	MultiApp V4.0.1 : AGD PRE document - eTravel v2.2, référence D1433280, version 1.0 du 26/6/2017, GEMALTO.	[CER]
	eTravel v2.2 and 2.3 Reference Manual, référence D1392378 du 26/3/2020, GEMALTO.	**[R-S01]**
	Global Dispatcher Personalization Applet User Guide, référence D1390286D du 30/5/2017, GEMALTO.	[CER]
	MultiApp V4.0.1 : AGD OPE document - eTravel v2.2, référence D1433279, version 1.0 du 26/6/2017, GEMALTO.	[CER]
	Rules for applications on Multiapp certified product, référence D1484823, version 1.2 de janvier 2019, GEMALTO.	**[R-S01]**
	Guidance for secure application development on Multiapp platforms, référence D1390326, version A01 de mars 2018, GEMALTO.	**[R-S01]**
	Verification process of *GEMALTO* non sensitive applet, référence D1484874, version 1.0 de décembre 2018, GEMALTO.	**[R-S01]**
	Verification process of Third Party non sensitive applet, référence D1484875, version 1.2 de février 2019, GEMALTO.	**[R-S01]**
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr..	[CER]