Compass Security AG
Werkstrasse 20
Case postale 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

SIX Terravis SA

Audit de la gestion fiduciaire

28 février 2014

Document source:	report_81872_terravis_partner_v1.3.docx
Version:	v1.3
Numéro du projet:	81872
Auteur(s):	Michael Fisler, Compass Security AG
Date de distribution:	28 février 2014
Classification:	PUBLIC

1 Management Summary

1.1 Evaluation globale

Sur la base des résultats de l'audit de sécurité effectué en octobre 2013 par la société Compass Security, la sécurité des services web «Nominee» de Terravis, de l'application web et de l'infrastructure a été jugée *satisfaisante*. Les analystes n'ont constaté aucune menace susceptible de porter atteinte à l'intégrité, à la disponibilité et à la confidentialité des données. Ils n'ont identifié que des vulnérabilités de faible et moyenne gravité qu'il convient de combler pour atteindre un niveau de sécurité élevé.

1.2 Introduction

En 2013, SIX Terravis SA a intégré une nouvelle fonction sur la plateforme en service, laquelle permet à SIX d'agir en tant que fiduciaire pour les inscriptions au registre foncier. Au printemps 2014, le système a été complété par une série de services web, qui permettent aux partenaires de communiquer directement avec le système. Dans le cadre d'une procédure de contrôle, Compass a réévalué la sécurité de la nouvelle fonctionnalité et des systèmes.

L'audit de sécurité avait pour but de brosser un tableau des menaces concrètes en provenance d'Internet. Les constats suivants ont notamment été élaborés:

- Estimation du potentiel de menace de l'architecture et de la connexion Internet en place du point de vue d'un pirate d'Internet
- Analyse des nouveaux services web en termes d'autorisation et d'authentification et vérification du traitement général des données saisies par les utilisateurs
- Nouvelle vérification des vulnérabilités constatées lors du test effectué en été 2013
- Recommandations détaillées visant à améliorer la sécurité

Les vulnérabilités identifiées en juin 2013 ont été traitées par les développeurs. Afin de s'assurer que les problèmes de sécurité ont été résolus, Compass a examiné une nouvelle fois l'application en février 2014.

1.3 Résultats

Tous les problèmes de sécurité des services web identifiés par Compass ont été traités au cours du projet et considérés comme résolus suite à un nouvel examen.

Il convient de noter que les données émises par les services web sont transmises à l'application de manière non codée. Les utilisateurs des services web doivent par conséquent veiller eux-mêmes à ce que les données entrantes soient correctement traitées. Dans le cas contraire, des attaques de type Cross-Site Scripting peuvent se produire et l'utilisateur peut, par exemple, être redirigé automatiquement vers un site web malveillant ou de hameçonnage (phishing).

Toutes les vulnérabilités graves de l'application web ont été éliminées. Seules des vulnérabilités de faible gravité restent à combler.

L'infrastructure et la configuration comportent encore des vulnérabilités de faible et moyenne gravité.

Compass Security AG
Werkstrasse 20
Case postale 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

1.4 Recommandations

Compass Security recommande d'éliminer dans une perspective de moyen terme les vulnérabilités de faible et moyenne gravité restantes.

Compass Security AG
Werkstrasse 20
Case postale 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch