SIX Terravis AG
Terravis Penetration Test

Quelldokument:	report_84013_Terravis_Partner_v1.0.docx
Version:	v1.0
Projektnummer:	84013
Auslieferungsdatum:	8. Februar 2017
Autoren:	Mirko Selber, Compass Security Schweiz AG Michael Fisler, Compass Security Schweiz AG
Klassifikation:	PUBLIC

Compass Security Schweiz AG, Werkstrasse 20, Postfach 2038, CH-8645 Jona
T +41 55 214 41 60, team.csch@compass-security.com, www.compass-security.com

1 Management Summary

1.1 Gesamtbeurteilung

Aufgrund der Ergebnisse des im Januar 2018 durchgeführten Penetrationstests beurteilt Compass Security die Sicherheit der Terravis-Applikation als gut. Die wichtigsten Punkte des vorherigen Assessments wurden korrekt adressiert. Die Analysten haben keine Bedrohungen festgestellt, die eine direkte signifikante Einschränkung der Vertraulichkeit, Integrität und Verfügbarkeit der Terravis Systeme und Information Assets zur Folge haben. Es wurden nur wenige mit mittel bis leicht gewichtete Schwachstellen identifiziert, die zur Erreichung eines sehr guten Sicherheitsniveaus behoben werden sollten.

1.2 Einleitung

SIX Terravis AG hat seit dem letzten Assessment durch Compass Security, welches im Dezember 2015 stattfand, die Terravis-Applikation weiter ausgebaut. Die bestehende Funktionalität wurde durch neue Prozesse erweitert, die eine 2-Augen oder 4-Augen Bestätigung von TrueSale Depots erlauben. Im Rahmen einer Abnahmeprüfung soll nun die Sicherheit der neuen Funktionalität beurteilt, sowie die adressierten Punkte aus den vorherigen Tests neu bewertet werden. Compass Security hat ein entsprechendes Assessment durchgeführt.

Die Sicherheitsüberprüfung diente dazu, einen Überblick über die externen vom Internet ausgehenden, konkreten Bedrohungen zu erhalten. Insbesondere wurden dabei folgende Erkenntnisse erarbeitet:

- Einschätzung des Bedrohungspotentials der implementierten Web-Anwendung, sowohl aus der Sicht eines anonymen Angreifers im Internet als auch eines authentisierten Benutzers.
- Analyse der neuen Funktionalität in Bezug mit Fokus auf die Autorisierung
- Recheck der bisher identifizierten Schwachstellen
- Detaillierte Empfehlungen zur Verbesserung der Sicherheit

1.3 Ergebnisse

Als Grundlage für die Applikation wird ein Framework benutzt, das viele Angriffe verunmöglicht oder zumindest stark erschwert. Die Kernfunktionalität der Terravis Applikation ist nur für authentisierte Benutzer erreichbar. Dadurch wird die Angriffsoberfläche klein gehalten. Die Authentifizierung ist mittels Zwei-Faktor-Authentifizierung gelöst, wodurch ein adäquater Schutz vor Account-Diebstählen gewährleistet werden kann.

In der Autorisierungsprüfung konnten keine Fehler identifiziert werden. Es war weder möglich, das 2-Augen oder 4-Augen Prinzip bei den TrueSale Depots zu unterwandern, noch konnten Funktionen ausgeführt werden, auf die der Benutzer keine Rechte hatte.

Zudem wurden die kritischsten Befunde aus dem letzten Test behoben. Die verwendeten Code-Bibliotheken nun auf dem neuesten Stand und haben somit keine bekannten Schwachstellen.

1.4 Empfehlungen

Compass Security empfiehlt, dass die verbleibenden, mittel und leicht gewichteten Schwachstellen mittelfristig ebenfalls behoben werden.