SIX Terravis AG
Terravis Penetration Test

Quelldokument:	report_84745_Terravis_Partner_v1.0.docx
Version:	v1.0
Projektnummer:	84013
Auslieferungsdatum:	13. März 2019
Autoren:	Urs Müller, 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 März 2019 während 5 Tagen auf der Testumgebung durchgeführten Penetrationstests beurteilt Compass Security die Sicherheit der Terravis-Applikation als gut. Die wichtigsten Punkte des vorherigen Assessments wurden korrekt adressiert. Es verbleiben keine Bedrohungen, die eine direkte signifikante Einschränkung der Vertraulichkeit, Integrität und Verfügbarkeit der Terravis Systeme und Information Assets zur Folge haben. Die wenigen mit leicht bewerteten Schwachstellen sollten zur Erreichung eines sehr guten Sicherheitsniveaus ebenfalls behoben werden.

1.2 Einleitung

SIX Terravis AG hat seit dem letzten Test durch Compass Security die Terravis-Applikation an vielen Stellen geändert oder ergänzt, ohne jedoch neue Funktionalität bereitzustellen. Im Rahmen einer wiederkehrenden Prüfung wurde nun die Sicherheit der gesamten Applikation nochmals stichprobenweise durch Compass Security analysiert, sowie die adressierten Punkte aus den vorherigen Tests neu bewertet.

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.
- Erneute Analyse der bestehenden Funktionalität
- 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.

Die Tests in bisher nicht abgedeckten Funktionalitäten haben Schwachstellen aufgezeigt, die jedoch noch während des Testzeitraums erfolgreich adressiert und von Compass Security als behoben bestätigt werden konnten.

Zudem wurden die kritischsten Befunde aus dem letzten Test behoben. So wurde die Nominee-Transfer Datei-Prüfung verbessert und ein aus dem Internet erreichbarer, nicht benötigter Service wurde abgeschaltet, um die Angriffsoberfläche weiter zu reduzieren.

1.4 Empfehlungen

Compass Security empfiehlt, dass die verbleibenden, leicht gewichteten Schwachstellen längerfristig ebenfalls behoben werden.