Gemeinsame Einrichtung KVG

SORA PCG

Date of Delivery: Dezember 12., 2019
Classification: PUBLIC STATEMENT

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 Zusammenfassung der Sicherheitsprüfung

Compass Security hat im Oktober und November 2019 während 8 Personentagen die Sicherheit der SORA PCG Applikation getestet. Die Tests wurden in einer produktiven Umgebung mit Testdaten durchgeführt.

1.1 Einleitung

SORA PCG soll die Global Trade Item Number (GTIN) inkl. Mengen und Kosten erheben und diese dann sicher und zeitnah an die Gemeinsame Einrichtung KVG übermitteln, damit der Risikoausgleich nach der neuen Verordnung Risikoausgleich (VORA) mit den Pharmaceutical Cost Group (PCG) zugeordnet werden und korrekt berechnet werden kann.

Compass Security Schweiz AG ist ein auf Security Assessments und forensische Untersuchungen spezialisiertes Unternehmen mit Hauptsitz in Jona SG und Filialen in Bern, Zürich, Berlin und Toronto. Im Auftrag des Kunden werden Penetrationstests und Security Reviews durchgeführt, um die IT-Sicherheit in Bezug auf Hacking-Attacken zu beurteilen sowie geeignete Massnahmen zur Verbesserung des Schutzes aufzuzeigen.

1.2 Ziele

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 SORA Applikation und der Web Services, sowohl aus der Sicht eines anonymen Angreifers im Internet als auch eines authentisierten Benutzers.
- Detaillierte Empfehlungen zur Verbesserung der Sicherheit.
- Überprüfung der daraufhin implementierten Korrekturen und Verbesserungen.

1.3 Zielsysteme

Die Resultate beziehen sich auf die SORA PCG Web Server inkl. Web Services, sowie die Electron Windows Applikation in Version 2.0.22, welche im Oktober und November 2019 getestet wurden.

1.4 Methodik

Die Ergebnisse der Penetrationstests wurden durch manuelles Hacking als registrierte und anonyme Benutzer erarbeitet. Ausserdem wurde der Quellcode zur Verfügung gestellt. (Gray-Box Ansatz). Dabei wurde die Applikation insbesondere in Bezug auf Security Best Practices und OWASP Top 10 analysiert.

1.5 Resultat

In der Applikation und den zugehörigen Web Services konnten lediglich geringfügige Schwachstellen identifiziert werden, die weder Einfluss auf Vertraulichkeit noch Integrität der Daten haben. Die Infrastruktur schützt sowohl Benutzer als auch Daten vor unbefugtem Zugriff und verarbeitet Benutzereingaben zuverlässig, so dass keine Manipulationen durchgeführt werden konnten. Diverse Security Best Practices wurden eingehalten. Als Folge dessen konnten durch den Test lediglich zusätzliche Empfehlungen ausgesprochen werden, um den ohnehin hohen Sicherheitsstandard noch weiter zu erhöhen.