Gemeinsame Einrichtung KVG

SORA PCG

Public Statement

17. Dezember 2021

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

Public Statement

Die Gemeinsame Einrichtung KVG veröffentlicht bis Ende des Jahres eine neue Version von SORA PCG. Im Dezember 2021 hat Compass Security Schweiz AG die Sicherheit der SORA PCG Applikation analysiert. Dieses Dokument gibt einen Überblick über die Resultate. Weitere technische Details wurden der Gemeinsamen Einrichtung KVG in einem separaten Dokument mitgeteilt.

Einführung

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 Schweizer IT-Sicherheitsunternehmen, das sich darauf spezialisiert hat, für Kunden qualitativ hochwertige, massgeschneiderte Security Assessments und forensische Untersuchungen durchzuführen. Gegründet 1999, verfügt Compass über mehr als 20 Jahre Erfahrung in nationalen und internationalen Projekten mit Fortune-500-Unternehmen, KMUs und Start-Ups aus den Bereichen Finanzen, Medizin, Industrie und Pharma. Die vielfältigen Ausbildungen und Vertiefungsrichtungen unserer Sicherheitsanalysten sowie die enge Zusammenarbeit mit führenden Schweizer Universitäten stellen sicher, dass unsere Analysten stets über die neuesten Entwicklungen in der Sicherheitsbranche informiert sind.

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.

Umfang

Das Security Assessment umfasste folgende Systeme:

Applikation / Zielsystem	Zeitraum	Aufwand
SORA PCG Windows Electron Applikation v2.5.13 SORA PCG Web Server & Web Services	06.12.2021 - 10.12.2021	4 PT

Es gilt zu beachten, dass sich sämtliche Aussagen in diesem Dokument ausschliesslich auf die oben aufgeführten Versionen/Daten beziehen.

Methodik

Die Ergebnisse der Penetrationstests wurden durch manuelle Sicherheitsanalysen 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 die OWASP Top 10 Bedrohungen analysiert.

Resultate

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.

Einschränkungen

Es gab keine Einschränkungen während dem Test.