

Mit der BRAK wurde der erneute Test der unten aufgeführten Schwachstellen aus der „Technische Analyse und Konzeptprüfung des beA“ - Abschlussgutachten - V1.0 vom 18.06.2018 vereinbart. Die Ergebnisse der ReTests (Stand 17.08.2017) sind nachfolgend dargestellt.

Kapitel 3.5.3 – Modifikation von signierten Nachrichten

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.1 – Veraltete Javascript-Bibliotheken in der beA-Anwendung

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.2 – Überschreiben von Dateien

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.3 – Session-ID als GET Parameter in der URL

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.7 – Detaillierte Fehlermeldungen der Webapplikationsfirewall

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.9 – Qualität der genutzten Session-Cookies

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.10 – Automatisches Ausführen und Öffnen von Dateien

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.12 – Logdaten: Detaillierte Struktur der REST-Endpunkte

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 3.6.13 – Nicht konsistente Zertifikatsprüfung

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 4.5.1 – SQL-Injection

Schwachstellenbehebung: **verifiziert, behoben**

Vom Gutachter wurde ein zusätzlich beauftragtes Quelltext-Audit durchgeführt. Die Angabe des Herstellers, die SQL-Injection-Schwachstelle sei bereits ausreichend bekämpft, konnte gutachterlich bestätigt werden.

Kapitel 4.5.2 – Initialisierungs-Vector

Schwachstellenbehebung: **verifiziert, behoben**

Kapitel 5.4.1 - Verwendung von Javascript beim beA-Client

Schwachstellenbehebung: **verifiziert, behoben**

Das vom Hersteller vorgelegte Konzept zur technischen Umsetzung wurde als hinreichend sicherer Lösungsvorschlag bewertet.

Kapitel 5.4.2 – Client prüft Postfachzertifikate nicht

Schwachstellenbehebung: **verifiziert, behoben**

Das von der BRAK dargestellte Konzept zur technischen Umsetzung wurde als hinreichend sicherer Lösungsvorschlag bewertet.