ZERTIFIKAT

Bestätigung der Informationssicherheit

Geltungsbereich:	ene't Navigator mit allen Apps ene't Navigator API
Testzeitraum:	Februar 2020
Ergebnis:	keine Schwachstellen

Die Webanwendung ene't Navigator (https://www.enet-navigator.de/) mit allen enthaltenen Apps sowie die zugehörige Web-API (https://api.enet-navigator.de/) wurde im Februar 2020 auf mögliche Schwachstellen hin überprüft.

Die Prüfung fand gemäß den Vorgaben des OWASP Web Application Testing Guide in der Version 4 statt.

Die Webanwendung ene't Navigator erfüllt alle geforderten Sicherheitsanforderungen.

Christian H. Gresser, CISSP, CEH Master

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Ergebnisse im Detail

A1:2017: Injection

Die Eingabefelder der Navigator Apps erlauben keine Injection-Angriffe. SQL-Befehle, Sonderzeichen und sonstige Varianten werden gefiltert bzw. maskiert.

A2:2017: Broken Authentication

Die Authentisierung ist korrekt umgesetzt. Anmeldeinformationen oder Session Cookies können nicht manipuliert werden, um unberechtigten Zugriff zu erhalten.

A3:2017: Sensitive Data Exposure

Ein Zugriff auf vertrauliche oder besonders schützenswerte Daten war nicht möglich. Die Belange des Datenschutzes sind umgesetzt.

A4:2017: XML External Entities (XXE)

Der XML-Parser zur Auswertung der JSON-Anfragen ließ sich nicht angreifen. Anfragen mit manipulierten oder fehlerhaften Parametern wurden korrekt zurückgewiesen und führten nicht zu einem fehlerhaften Verhalten.

A5:2017: Broken Access Control

Zugriffsberechtigungen werden korrekt eingehalten. Ein Zugriff auf Daten anderer Accounts war nicht möglich.

A6:2017: Security Misconfiguration

Der Webserver und die Webanwendung sind soweit im Penetrationstest überprüfbar, sicher konfiguriert. Der Webserver unterstützt starke Verschlüsselung mit aktuellen TLS-Versionen, schwache Verschlüsselungsparameter werden nicht angeboten.

A7:2017: Cross-Site Scripting (XSS)

Cross-Site Scripting Angriffe waren nicht erfolgreich. Alle Sonderzeichen wurden korrekt und vollständig maskiert.

A8:2017: Insecure Deserialization

Bei der Verarbeitung übergebener Parameter wurden keine Fehler identifiziert.

A9:2017: Using Components with Known Vulnerabilities

Der eingesetzte Webserver sowie genutzte Bibliotheken enthalten, soweit im Penetrationstest identifizierbar, keine bekannten Sicherheitslücken.

A10:2017: Insufficient Logging & Monitoring

Zugriffe auf die Webanwendung werden mitprotokolliert und ausgewertet. Die durchgeführten Angriffe wurden erkannt und gemeldet.