PUBLIC
– distributed at EnerKey Oy's discretion

elfgroup

EnerKey Oy

Security Evaluation of the EnerKey Portal

Public Summary Statement

Issued July 17th, 2020

elfGROUP Cyber Security Services Ltd / FI31094425
Hiltusentie 23 A 1, FI-90620 OULU, Finland
elfgroup.fi

Security Assessment Summary Statement

elfGROUP Cyber Security Services Ltd conducted a comprehensive security assessment and a web application and API level penetration testing of EnerKey Oy's EnerKey Portal – an energy management platform for optimizing buildings' energy efficiency. The assessment included a thorough review of the solution architecture, development practices and the used toolchain as well as a black-box penetration testing of the web application and its API interfaces.

Based on the documentation reviews done and the solution expert interviews conducted during the architecture review workshop, we conclude that the architectural decisions made and the software implementation are deemed to be in a very good shape in light of common cyber security best practices.

During the July 2020 testing period, the application and its API interfaces were thoroughly tested according to industry accepted security recommendations and checklists, including but not limited to the OWASP guidelines for testing authentication, request and access authorization, input validation, data integrity controls, data access controls and hosting platform security misconfiguration issues.

At the time of the CyberSafe Solution certification, no critical or high security issues were present in the application. The EnerKey Portal platform is considered to be adequately protected for storing enterprise sensitive data and personally identifiable information (PII), taking into account its intended use, environment and the expected risk landscape.

As a minimum, thorough annual re-testing is suggested with smaller refresh test rounds every six months in order to keep up with threat evolution and security patches.

Certificate: #2007-S1-d98617763

EnerKey Portal
CyberSafe Certified Solution

Date: July 17th, 2020 (first issue)
Target: EnerKey Portal (https://*.enerkey.com)
Testing timeframe: July 2020
Issues: Critical: No, High: No
Validity: July 31st, 2021

https://www.elfgroup.fi/ecc/2007-S1-d98617763.pdf

ECC/S Certificate #2007-S1-d98617763

elfGROUP Cyber Security Services Ltd / FI31094425
Hiltusentie 23 A 1, FI-90620 OULU, Finland
elfgroup.fi

Importance of recurring security testing

Please keep in mind that any security evaluation and testing effort measures and reports the level of security at the time of the actual testing and system evaluation. The entire server stack from the front-most load balancers to the persistence and backend API layers, as well as all application components and connected systems, contribute to the overall security posture of the target platform.

Any changes made to the test subject or its runtime environment may change the level of effective security to an extent that can be only determined with recurring security testing. Furthermore, even changes to the surrounding peer servers with physical connectivity to the target environment can affect the level of effective protection. Especially in a public cloud infrastructure, there is essentially no perimeter protection anymore and the horizontal threats from peer servers are to be taken seriously. Public cloud infrastructures are also subject to constant, unannounced modification.

External actors and the development of the field in general affect each information system's security posture over time. New vulnerabilities are constantly found and disclosed in server and client products, often making applications and their data more exposed to the public. Exploits using found vulnerabilities spread quickly and the tools to utilize them become increasingly commonplace. Additionally, commodity hardware and peer networks enable brute-force and denial-of-service attacks that are a substantial threat for a service of any scale.

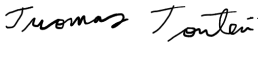
Security work has to be a continuous proces. Security testing is always performed with the current timely knowledge of published vulnerabilities, exploitation techniques and the server and application software versions deployed on the target servers. Few months, half a year, later the web application security landscape has evolved, vendors have updated their software packages and new vulnerabilities have gone through disclosure process, becoming common knowledge for script kiddies, professional hackers and cyber-terrorists world-wide.

For this reason, continued testing is an important part of any corporation's security process.

All elfGROUP auditors and security testers assigned to this assessment are skilled professionals and we are not aware of anything that might have impaired their independence or impartiality on this assessment.

Thank you for trusting elfGROUP.

Tuomas Tonteri, Senior Security Architect (CISSP, CISA, CSM)
Markus Hamara, Chief Cyber Security Analyst (ISO 27001 Lead Auditor)
Miika Rinne, Senior Cyber Security Analyst (OSCP, CRTP)



elfGROUP Cyber Security Services Ltd / FI31094425
Hiltusentie 23 A 1, FI-90620 OULU, Finland
elfgroup.fi