elfgroup

Docue Technologies Oy

Security Evaluation of Sopimustieto.fi

Public Summary Statement

Renewed December 17th, 2020
First issued September 9th, 2019

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

Sopimustieto.fi – Security Assessment Summary Statement

elfGROUP Cyber Security Services Ltd was contracted by Docue Technologies Oy in November 2020 to conduct a security assessment and penetration testing of their web application Sopimustieto.fi. This cyber security assessment was set to evaluate the overall level of the web application's and its cloud hosting environment's security level.

The application was tested for common web application vulnerabilities such as cross-site scripting (XSS), cross-site request forgery (CSRF), authentication and authorization problems, server misconfiguration, SQL injection and various other exploits. For example, the OWASP Top 10 Web application security vulnerabilities list was covered in full. The main focus was put on ensuring that access controls are fully effective ensuring that customers' data stored within the application remains confidential and integral. In addition to the application security verification, the cloud hosting environment was comprehensively reviewed for best security governance practices and hardened configuration.

elfGROUP was provided with various user accounts of different access levels to the target system. During the testing period, the web application's business logic, access controls and all visible backend interfaces were thoroughly tested according to well known security recommendations and checklists, including the OWASP Testing Guide, Web Service Security Testing and REST Security guidelines.

No critical or high security issues were discovered. The Sopimustieto.fi application is considered to be adequately protected taking into account its intended use and the risk landscape. As a minimum, thorough annual re-testing is suggested in order to keep up with threat evolution and security patches.

Certificate: #1909-S1-37d54da76

Sopimustieto.fi
CyberSafe Certified Solution

Date: December 17th, 2020 (originally issued September 9th, 2019)
Target: Sopimustieto.fi web application
Testing timeframe: November 2020
Issues: Critical: No, High: No
Validity: December 31st, 2021

https://www.elfgroup.fi/ecc/1909-S1-37d54da76.pdf

ECC/S Certificate #1909-S1-37d54da76

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.

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 process. 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

Henrik Mourujärvi, Penetration Tester

Markus Hamara, Senior Cyber Security Analyst, ISO 27001 ISMS Auditor

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