elfgroup

Aiven Oy

Security Evaluation of Managed Cloud Services

Public Summary Statement

Renewed August 30th, 2019
First issued August 4th, 2017

elfGROUP Cyber Security Services Ltd / FI23540122
Hiltusentie 23 A 1, FI-90620 OULU, Finland
elfgroup.fi

Aiven.io – Security Assessment Summary Statement

elfGROUP Cyber Security Services Ltd was contracted by Aiven Oy in June 2019 to conduct a security assessment and penetration testing of their managed cloud service hosting platform, Aiven.io. This cyber security assessment was set to evaluate the overall service infrastructure including the Aiven.io management console and its public facing programming interfaces, APIs.

The main focus was put on assuring the security of the public REST Management API that not only provides an external integration point but also implements the core functionality under the hood for the web based management console. Another critical target was to ensure that the end customers' cloud service instances cannot be exploited or broken out of to enable any sort of privilege escalation or to be able to access or manipulate other users' cloud instances.

elfGROUP was given system-wide access to a separated test environment that was an identical copy of the production environment, including Aiven.io's backend services. During the two month testing period, the service management web console, API interfaces and the inner technical service instantation, deployment and governance functionality was thoroughly tested according to well known security recommendations and checklists, including OWASP Testing Guide, Web Service Security Testing and REST Security guidelines.

Additionally to the application and API testing, the platform's server infrastructure including application, management and persistence layer servers, was assessed for proper secure and fail-safe configuration, strong and modern protective measures and use of ciphers and key strengths currently deemed to provide a very good level of data privacy.

No critical or high security issues were discovered. The Aiven.io platform 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 with smaller refresh test rounds every 3-6 months in order to keep up with threat evolution and security patches.

Certificate: #1708-S6-71acd0046

Aiven.io
CyberSafe Certified Solution

Date: August 30th, 2019 (originally issued August 4th, 2017)
Target: Aiven.io Managed Cloud Service Hosting
Testing timeframe: June / 2019
Issues: Critical: No, High: No, Medium: 2
Validity: August 31st, 2020

https://www.elfgroup.fi/ecc/1708-S6-71acd0046.pdf

ECC/S Certificate #1708-S6-71acd0046

elfGROUP Cyber Security Services Ltd / FI23540122
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
Miika Rinne, Cyber Security Analyst, OSCP
Edward Shornock, Cyber Security Expert, Infra Specialist

elfGROUP Cyber Security Services Ltd / FI23540122
Hiltusentie 23 A 1, FI-90620 OULU, Finland
elfgroup.fi