Leviathan Security Group, Inc.
3223 3rd Ave S., Suite 100
Seattle, WA 98134

Aiven Oy
Antinkatu 1, 6th Floor
00100 Helsinki
Finland

5 August 2022

To: James Arlen, CISO

RE: Aiven Postgres Gateway module

As of 7 July, 2022, Leviathan completed a security assessment of the Aiven Postgres Gateway module. We confirm that our testing occurred from 5 July, 2022 through 7 July, 2022, with a retest performed on August 3rd, 2022. We identified no malicious or extraneous functionality in the Gateway module. Three items were found that could be improved upon but did not represent a security risk. These items were remediated by the Aiven team and we validated the fixes with the retest described above.

We reviewed the code, build configuration, and compiled library. The purpose of the engagement was to identify any malicious or extraneous functionality within the Aiven Postgres Gateway during the time allocated to us. Leviathan used automated and manual testing guided by associated documentation.

As part of this assessment, Leviathan evaluated the code for the following characteristics:

- Code contains no extraneous or malicious functionality
- Coding best practices
- Bounds checking and safe memory access
- Type correctness
- Memory management
- Race conditions
- Absence of insecure functions
- Absence of logical vulnerabilities

The three minor issues identified and remediated corresponded to coding best practices but did not constitute any vulnerability or exploit in the code.

This letter is valid for the Aiven Postgres Gateway module as it appeared at commit "b2c7a4a60d20f67984b6325cb6426cce671135cf" during the testing window. Please direct any questions regarding this assessment to Alex Muentz, COO, Leviathan Security Group.
Signed,

Alexander Muentz
Chief Operating Officer
Leviathan Security Group