Security

 › [Administration](https://grafana.com/docs/grafana/latest/administration/) › Security

If you run non-Grafana web services on your Grafana server or within its local network, then they might be vulnerable to exploitation through the Grafana data source proxy or other methods.

如果在你的Grafana服务器或它的本地网络中去运行非Grafana网站服务，那么它们可能通过Grafana数据源或其他方式受到攻击利用。

To prevent this type of exploitation from happening, we recommend that you apply one or more of the precautions listed below.

去预防这种类型的用户发生，我们建议你使用下面列出来的几种预防措施。

Limit IP addresses/hostnames for data source URL

对于数据源URL进行IP地址或主机名限制

You can configure Grafana to only allow certain IP addresses or hostnames to be used as data source URLs and proxied through the Grafana data source proxy. Refer to [data\_source\_proxy\_whitelist](https://grafana.com/docs/grafana/latest/administration/configuration/#data-source-proxy-whitelist) for usage instructions.

你可以配置Grafana，只允许当前的IP地址或主机名做为数据源的URL和Grafana的数据源代理。到data\_source\_proxy\_whitelist了解使用介绍。

Firewall rules

防火墙规则

Configure a firewall to restrict Grafana from making network requests to sensitive internal web services.

配置一个防火墙来限制外部网络服务的敏感请求。

There are many firewall tools available, refer to the documentation for your specific security tool. For example, Linux users can use [iptables](https://en.wikipedia.org/wiki/Iptables).

有很多防火墙工具可用，参考你指定的安全工具的文档来了解。例如，Linux用户可以使用iptables。

Proxy server

Require all network requests being made by Grafana to go through a proxy server.

所有的网络请求都会经过Grafana代理服务。

Limit Viewer query permissions

限制观察者的查询权限

Users with the Viewer role can enter *any possible query* in *any* of the data sources available in the **organization**, not just the queries that are defined on the dashboards for which the user has Viewer permissions.

观察者用户可以在组织中可用的任何数据源中输入任何可能的查询，而不仅仅是在有权限的Dashboard上查看定义好的查询。

**For example:** In a Grafana instance with one data source, one dashboard, and one panel that has one query defined, you might assume that a Viewer can only see the result of the query defined in that panel. Actually, the Viewer has access to send any query to the data source. With a command-line tool like curl (there are lots of tools for this), the Viewer can make their own query to the data source and potentially access sensitive data.

例如：在一个Grafana实例中，这个实例有一个数据源，一个Dashboard，一个带有一个查询定义的面板，假设你是一个观察者，只能查看面板上定义好的查询结果。实际上，观察者有发送任何查询到数据源的权限。使用像curl这样的命令行工具（有很多同样的工具），观察者可以查询数据源中的数据，或可能访问敏感数据。

To address this vulnerability, you can restrict data source query access in the following ways:

想要解决这种易受攻击的现象，你可以使用以下方法来限制数据源的查询权限：

* Create multiple data sources with some restrictions added in data source config that restrict access (like database name or credentials). Then use the [Data Source Permissions](https://grafana.com/docs/grafana/latest/permissions/datasource_permissions/) Enterprise feature to restrict user access to the data source in Grafana.

创建多个具有一些权限的数据源，添加到数据源配置中限制权限（像数据库名字或证书）。然后使用数据源权限企业版功能去限制用户访问数据源。

* Create a separate Grafana organization, and in that organization, create a separate data source. Make sure the data source has some option/user/credentials setting that limits access to a subset of the data. Not all data sources have an option to limit access.

创建一个隔离的Grafana组织，在这个组织中再创建一个隔离的数据源。确保数据源中有一些选项/用户/证书设置来限制访问数据的子集。不是所有的数据源都有一个选项去限制访问。