# CVE-2022-21702: Grafana proxy XSS

Moderate **vtorosyan** published **GHSA-xc3p-28hw-q24g** on Feb 8

Package

**datasource and plugin proxy** (Grafana)

| Affected versions | Patched versions |
|---|---|
| 2.0.0-beta1 - 8.3.4 | 8.3.5, 7.5.15 |

**Description**

Today we are releasing Grafana 8.3.5 and 7.5.15. This patch release includes MEDIUM severity security fix for XSS for Grafana.

Release v.8.3.5, only containing security fixes:

- Download Grafana 8.3.5
- Release notes

Release v.7.5.15, only containing security fixes:

- Download Grafana 7.5.15
- Release notes

## XSS (CVE-2022-21702)

### Summary

On Jan. 16, an external security researcher, Jasu Viding contacted Grafana to disclose an XSS vulnerability in the way that Grafana handles data sources.

An attacker could serve HTML content through the Grafana datasource or plugin proxy and trick a user to visit this HTML page using a specially crafted link and execute a Cross-site Scripting (XSS) attack. The attacker could either compromise an existing datasource for a specific Grafana instance or either set up its own public service and instruct anyone to set it up in their Grafana instance.

We believe that this vulnerability is rated at CVSS 6.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N).

## Impact

Should an existing data source connected to Grafana be compromised, it could be used to inappropriately gain access to other data sources connected to the same Grafana org.

## Affected versions with MEDIUM severity

To be impacted, all of the following must be applicable:

**For data source proxy**:

- A Grafana instance running version v2.0.0-beta1 up to v8.3.4.
- A Grafana HTTP-based datasource configured with Server as Access Mode and a URL set.
- Attacker to be in control of the HTTP server serving the URL of above data source.
- A specially crafted link pointing at http://host/api/datasources/proxy/"data source id" and attacker somehow tricks a user of the above Grafana instance to click/visit the link.
- A user that's already authenticated to above Grafana instance clicks on/visits the specially crafted link sent/provided by the attacker.

**For plugin proxy**:

- A Grafana instance running version v2.0.0-beta1 up to v8.3.4.
- A Grafana HTTP-based app plugin configured and enabled with a URL set.
- Attacker to be in control of the HTTP server serving the URL of above app.
- A specially crafted link pointing at http://host/api/plugin-proxy/"plugin id" and attacker somehow tricks a user of the above Grafana instance to click/visit the link.
- A user that's already authenticated to above Grafana instance clicks on/visits the specially crafted link sent/provided by the attacker.

**Backend plugin resource**:

- A Grafana instance running version v7.0.0-beta1 up to v8.3.4.
- Attacker potentially needs to craft a custom plugin to be able to pull this off, but if an attacker can compromise/control the backend service that a backend plugin connects to, it might be possible to serve HTML content via the /api/plugins/"plugin Id"/resources* or /api/datasources/"id"/resources* routes.
- A specially crafted link pointing at /api/plugins/"plugin Id">/resources* or /api/datasources/"id"/resources* and attacker somehow tricks a user of the above Grafana instance to click/visit the link.
- A user that's already authenticated to above Grafana instance clicks on/visits the specially crafted link sent/provided by the attacker.

## Root Causes

**Trigger**

Reproduced and confirmed via this Golang app:

```
package main

import (
        "fmt"
        "log"
        "net/http"
)

func main() {
        http.HandleFunc("/", func(w http.ResponseWriter, r *http.Request) {
                fmt.Fprintf(w, "<html><body><script>alert('XSS');</script></body></html>")
        })

        log.Fatal(http.ListenAndServe(":3011", nil))
}
```

A Prometheus datasource is configured in Grafana with URL http://localhost:3011.

When visitining http://localhost:3000/api/datasources/proxy/170 the scripts declared in the HTML page executes. Confirmed in both Chrome and Firefox.

## Solutions and mitigations

All installations between Grafana v2.0.0-beta1 up to v8.3.4 should be upgraded as soon as possible.

### Workarounds

Using a proxy, set a response header Content Security Policy: sandbox for the following routes:

```
/api/datasources/proxy*
/api/plugin-proxy*
/api/plugins/<pluginId>/resources*
/api/datasources/<id>/resources*
```

Another possible mitigation is setting the response header Content-Disposition: attachment; “proxy.txt”. Confirmed in both Chrome and Firefox.

## Timeline and postmortem

Here is a detailed timeline starting from when we originally learned of the issue. All times in UTC.

- 2022-01-16 16:19 Issue submitted by Jasu Viding
- 2022-01-17 14:40 CVSS score confirmed 6.8 at maximum and MEDIUM impact
- 2022-01-17 15:15 Vulnerability confirmed reproducible
- 2022-01-17 16:01 Begin mitigation for Grafana Cloud
- 2022-01-18 15:12 Similar report received

- 2022-01-19 09:57 CVE requested
- 2022-01-19 13:21 PR with fix opened
- 2022-01-19 19:53 GitHub issues CVE-2022-21702
- 2022-01-20 12:43 Second similar report received
- 2022-01-21 14:30 Private release planned for 2022-01-25, and public release planned for 2022-02-01
- 2022-01-25 12:00 Private release with patches
- 2022-02-01 12:00 During the public release process, we realized that private 7.x release was incomplete. Abort public release, send second private release to customers using 7.x
- 2022-02-08 13:00 Public release

### Acknowledgement

We would like to thank Jasu Viding for responsibly disclosing the vulnerability.

### Reporting security issues

If you think you have found a security vulnerability, please send a report to security@grafana.com. This address can be used for all of Grafana Labs' open source and commercial products (including, but not limited to Grafana, Grafana Cloud, Grafana Enterprise, and grafana.com). We can accept only vulnerability reports at this address. We would prefer that you encrypt your message to us by using our PGP key. The key fingerprint is

F988 7BEA 027A 049F AE8E 5CAA D125 8932 BE24 C5CA

The key is available from keyserver.ubuntu.com.

### Security announcements

We maintain a security category on our blog, where we will always post a summary, remediation, and mitigation details for any patch containing security fixes.

You can also subscribe to our RSS feed.

Severity

Moderate 6.8 / 10

CVSS base metrics

| | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | Low |
| User interaction | Required |
| Scope | Changed |

| | |
|---|---|
| Confidentiality | **High** |
| Integrity | **None** |
| Availability | **None** |

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N

### CVE ID

CVE-2022-21702

### Weaknesses

No CWEs