Grafana 8.3.1, 8.2.7, 8.1.8, and 8.0.7 released with high severity security fix

Vardan Torosyan • 2021-12-07 • 3 min

Note: *We released fixes for CVE-2021-41090 and CVE-2021-43798 within 24 hours and mixed them up in one of the three blog posts. To make it clear: CVE-2021-41090 is for the Grafana* ***Agent*** *and CVE-2021-43798 is for Grafana* ***the software****. Only CVE-2021-43798 was a 0day exploit.*

Today we are releasing Grafana 8.3.1, 8.2.7, 8.1.8, and 8.0.7. This patch release includes a high severity security fix that affects Grafana versions from v8.0.0-beta1 through v8.3.0.

Release v8.3.1, only containing a security fix:

- Download Grafana 8.3.1
- Release notes

Release v8.2.7, only containing a security fix:

- Download Grafana 8.2.7
- Release notes

Release v8.1.8, only containing a security fix:

- Download Grafana 8.1.8
- Release notes

Release v8.0.7, only containing a security fix:

- Download Grafana 8.0.7
- Release notes

Path Traversal (CVE-2021-43798)

On 2021-12-03, we received a report that Grafana is vulnerable to directory traversal, allowing access to local files. We have confirmed this for versions v8.0.0-beta1 to v8.3.0. Thanks to our defense-in-depth approach, at no time has Grafana Cloud been vulnerable.

The vulnerable URL path is: <grafana_host_url>*/public/plugins/<“plugin-id”>* where *<“plugin-id”>* is the plugin ID for any installed plugin.

Every Grafana instance comes with pre-installed plugins like the Prometheus plugin or MySQL plugin so the following URLs are vulnerable for every instance:

- <grafana_host_url>/public/plugins/alertlist/
- <grafana_host_url>/public/plugins/annolist/
- <grafana_host_url>/public/plugins/barchart/
- <grafana_host_url>/public/plugins/bargauge/
- <grafana_host_url>/public/plugins/candlestick/
- <grafana_host_url>/public/plugins/cloudwatch/
- <grafana_host_url>/public/plugins/dashlist/
- <grafana_host_url>/public/plugins/elasticsearch/
- <grafana_host_url>/public/plugins/gauge/
- <grafana_host_url>/public/plugins/geomap/
- <grafana_host_url>/public/plugins/gettingstarted/
- <grafana_host_url>/public/plugins/grafana-azure-monitor-datasource/
- <grafana_host_url>/public/plugins/graph/
- <grafana_host_url>/public/plugins/heatmap/
- <grafana_host_url>/public/plugins/histogram/
- <grafana_host_url>/public/plugins/influxdb/
- <grafana_host_url>/public/plugins/jaeger/
- <grafana_host_url>/public/plugins/logs/
- <grafana_host_url>/public/plugins/loki/
- <grafana_host_url>/public/plugins/mssql/
- <grafana_host_url>/public/plugins/mysql/
- <grafana_host_url>/public/plugins/news/
- <grafana_host_url>/public/plugins/nodeGraph/
- <grafana_host_url>/public/plugins/opentsdb
- <grafana_host_url>/public/plugins/piechart/
- <grafana_host_url>/public/plugins/pluginlist/
- <grafana_host_url>/public/plugins/postgres/
- <grafana_host_url>/public/plugins/prometheus/
- <grafana_host_url>/public/plugins/stackdriver/
- <grafana_host_url>/public/plugins/stat/
- <grafana_host_url>/public/plugins/state-timeline/
- <grafana_host_url>/public/plugins/status-history/
- <grafana_host_url>/public/plugins/table/
- <grafana_host_url>/public/plugins/table-old/
- <grafana_host_url>/public/plugins/tempo/
- <grafana_host_url>/public/plugins/testdata/
- <grafana_host_url>/public/plugins/text/
- <grafana_host_url>/public/plugins/timeseries/
- <grafana_host_url>/public/plugins/welcome/
- <grafana_host_url>/public/plugins/zipkin/

We have received CVE-2021-43798 for this issue. The CVSS score for this vulnerability is 7.5 High (CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) for Grafana versions 8.0.0-beta1 to 8.3.0

Affected versions with high severity

Solutions and mitigations

All installations between v8.0.0-beta1 and v8.3.0 should be upgraded as soon as possible.

If you cannot upgrade, running a reverse proxy in front of Grafana that normalizes the PATH of the request will mitigate the vulnerability. For example, the normalize_path setting in envoy.

Thanks to our defense-in-depth approach, Grafana Cloud instances have not been affected by the vulnerability.

As always, we closely coordinated with all cloud providers licensed to offer Grafana Pro. They have received early notification under embargo and confirmed that their offerings are secure at the time of this announcement. In alphabetical order, this is applicable to Amazon Managed Grafana and Azure Managed Grafana.

Timeline and postmortem

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

- 2021-12-03: Security researcher sends the initial report
- 2021-12-03: Confirmed for 8.0.0-beta1 through 8.3.0
- 2021-12-03: Confirmed that Grafana Cloud is not vulnerable
- 2021-12-03: Security fix determined and committed to Git
- 2021-12-03: Release timeline determined: 2021-12-07 for private customer release, 2021-12-14 for public release
- 2021-12-06: Second report about the vulnerability received
- 2021-12-07: We received information that the vulnerability has been leaked to the public, turning it into a 0day
- 2021-12-07: Decision made to release as quickly as feasible
- 2021-12-07: Private release with reduced 2-hour grace period, not the usual 1-week timeframe
- 2021-12-07: Public release

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.

Related content

Alexa Vargas Ortega · 31 Oct 2024 · 10 min read

Grafana dashboards are now powered by Scenes: big changes, same UI

Dashboard Grafana

Ronald McCollam · 30 Oct 2024 · 12 min read

Grafana variables: what they are and how they create dynamic dashboards

Dashboard Grafana Visualization

Malcolm Holmes · 29 Oct 2024 · 11 min read

Edit your Git-based Grafana dashboards locally

Grafana Dashboard

Sign up for Grafana stack updates

Email

Subscribe

Note: By signing up, you agree to be emailed related product-level information.

Grafana Labs

Grafana

Overview

Deployment options

Plugins

Dashboards

Products

Grafana Cloud

Grafana Cloud Status

Grafana Enterprise Stack

AI/ML tools for observability

Contextual root cause analysis | Grafana Cloud Asserts

Grafana Cloud Application Observability

Grafana Cloud Frontend Observability

Grafana Cloud k6

Grafana Cloud Logs

Grafana Cloud Metrics

Grafana Cloud Profiles

Grafana Cloud

Open Source

Grafana

Grafana Loki

Grafana Mimir

Grafana OnCall

Grafana Tempo

Grafana Agent

Grafana Alloy

Grafana k6

Prometheus

Grafana Faro

Grafana Pyroscope

Grafana Beyla

OpenTelemetry

Grafana Tanka

Graphite

GitHub

Learn

Grafana Labs blog

Documentation

Downloads

Community

Community forums

Community Slack

Grafana Champions

Community organizers

ObservabilityCON

GrafanaCON

The Golden Grot Awards

Successes

Workshops

Videos

OSS vs Cloud

Load testing

Log monitoring

Company

The team

Press

Careers

Partnerships

Contact Us | Grafana Labs

Getting help

Merch

Localized content

Japanese pages

German pages

French pages

Spanish pages

Portuguese pages

Grafana Labs uses cookies for the normal operation of this website. **Learn more.**

Grafana SLO

Grafana Cloud Status

Legal and Security Terms of Service Privacy Policy Trademark Policy