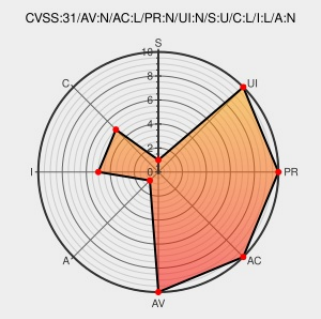
CVE-2021-41090

Published on: 12/08/2021 12:00:00 AM UTC

Last Modified on: 03/31/2022 04:30:00 PM UTC

CVE-2021-41090 - advisory for GHSA-9c4x-5hgq-q3wh

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Agent from Grafana contain the following vulnerability:

Grafana Agent is a telemetry collector for sending metrics, logs, and trace data to the opinionated Grafana observability stack. Prior to versions 0.20.1 and 0.21.2, inline secrets defined within a metrics instance config are exposed in plaintext over two endpoints: metrics instance configs defined in the base YAML file are exposed at `/-/config` and metrics instance configs defined for the scraping service are exposed at `/agent/api/v1/configs/:key`. Inline secrets will be exposed to anyone being able to reach these endpoints. If HTTPS with client authentication is not configured, these endpoints are accessible to unauthenticated users. Secrets found in these sections are used for delivering metrics to a Prometheus Remote Write system, authenticating against a system for discovering Prometheus targets, and authenticating against a system for collecting metrics. This does not apply for non-inlined secrets, such as `*_file` based secrets. This issue is patched in Grafana Agent versions 0.20.1 and 0.21.2. A few workarounds are available. Users who cannot upgrade should use non-inline secrets where possible. Users may also desire to restrict API access to Grafana Agent with some combination of restricting the network interfaces Grafana Agent listens on through `http_listen_address` in the `server` block, configuring Grafana Agent to use HTTPS with client authentication, and/or using firewall rules to restrict external access to Grafana Agent's API.

CVE-2021-41090 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **grafana** - **agent** version **>= 0.14.0, < 0.20.1**

Affected Vendor/Software: **grafana** - **agent** version **>= 0.21.0, < 0.21.2**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
announce patch releases by rfratto · Pull Request #1152 · grafana/agent · GitHub	github.com text/html	MISC github.com/grafana/agent/pull/1152
Release v0.20.1 · grafana/agent · GitHub	github.com text/html	MISC github.com/grafana/agent/releases/tag/v0.20.1
announce patch releases for cve-2021-41090 (#1152) · grafana/agent@af7fb01 · GitHub	github.com text/html	MISC github.com/grafana/agent/commit/af7fb01e31fe2d389e5f1c36b399ddc46b412b21
Inline secrets exposure · Advisory · grafana/agent · GitHub	github.com text/html	CONFIRM github.com/grafana/agent/security/advisories/GHSA-9c4x-5hgq-q3wh
Release v0.21.2 · grafana/agent · GitHub	github.com text/html	MISC github.com/grafana/agent/releases/tag/v0.21.2
December 2021 Grafana Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20211229-0004/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grafana	Agent	All	All	All	All

cpe:2.3:a:grafana:agent:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41090 : #Grafana Agent is a telemetry collector for sending metrics, logs, and trace data to the opinionat… twitter.com/i/web/status/1…	2021-12-08 16:20:18
@feedpushr	An update on 0day CVE-2021-41090: Grafana directory traversal grafana.com/blog/2021/12/0…	2021-12-08 16:42:17
/r/netcve	CVE-2021-41090	2021-12-08 17:38:34

← Previous ID

Next ID→