

CVE-2021-39226

Grafana Labs Grafana Authentication Bypass Vulnerability

CISA KEV since Aug 25, 2022

Actively exploited

Grafana is an open source data visualization platform. In affected versions unauthenticated and authenticated users are able to view the snapshot with the lowest database key by accessing the literal paths: /dashboard/snapshot/:key, or /api/snapshots/:key. If the snapshot "public_mode" configuration setting is set to true (vs default of false), unauthenticated users are able to delete the snapshot with the lowest database key by accessing the literal path: /api/snapshots-delete/:deleteKey.

EVRS 84 /100 Urgent priority	CVSS V3.1 7.3 High · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Sep 15, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Regardless of the snapshot "public_mode" setting, authenticated users are able to delete the snapshot with the lowest database key by accessing the literal paths: /api/snapshots/:key, or /api/snapshots-delete/:deleteKey. The combination of deletion and viewing enables a complete walk through all snapshot data while resulting in complete snapshot data loss. This issue has been resolved in versions 8.1.6 and 7.5.11. If for some reason you cannot upgrade you can use a reverse proxy or similar to block access to the literal paths: /api/snapshots/:key, /api/snapshots-delete/:deleteKey, /dashboard/snapshot/:key, and /api/snapshots/:key. They have no normal function and can be disabled without side effects.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
github.com/grafana/grafana	< 7.5.11	7.5.11	GitHub
github.com/grafana/grafana	≥ 8.0.0, < 8.1.6	8.1.6	GitHub
grafana	< 7.5.11 ≥ 8.0.0 < 8.1.6	7.5.11 · 8.1.6	NVD
fedora	34 35	no fixed version listed	NVD

Sources

Vendor guidance	github.com/grafana/grafana/commit/2d456a6375855364d098ede379438bf7f0667269	Additional guidance	github.com/grafana/grafana/security/advisories/GHSA-69j6-29vr-p3j9
grafana.com	grafana.com/blog/2021/10/05/grafana-7.5.11-and-8.1.6-released-with-critical-security-fix/	NVD	nvd.nist.gov/vuln/detail/CVE-2021-39226
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-69j6-29vr-p3j9
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-2169	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-39226

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.