



CVE-2023-0594

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-0594
State	PUBLIC
Assigner	security@grafana.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-01 16:15:00 UTC
Updated	2023-11-07 04:00:00 UTC
Description	Grafana is an open-source platform for monitoring and observability. Starting with the 7.0 branch, Grafana had a stored XSS vulnerability. An attacker could craft a malicious request to the /api/health endpoint, which would be processed by the server and result in a 500 Internal Server Error response. This vulnerability could be exploited to cause a Denial of Service (DoS) attack on the Grafana instance.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
404 Page not found Grafana Labs	MISC	grafana.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150659](#) Grafana Multiple Stored Cross-Site Scripting Vulnerabilities (CVE-2023-0594,CVE-2023-0507)

[691078](#) Free Berkeley Software Distribution (FreeBSD) Security Update for grafana (e7841611-b808-11ed-b695-6c3be5272acd)

[730754](#) Grafana Stored Cross-Site Scripting (XSS) Vulnerability

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report