



CVE-2019-19499

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2019-19499 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-08-28 15:15:00 UTC |
| Updated | 2022-04-28 18:28:00 UTC |
| Description | Grafana <= 6.4.3 has an Arbitrary File Read vulnerability, which could be exploited by an authenticated attacker that has pr |

Risk And Classification

Problem Types: CWE-89

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 |
|---|---------|---|------------------|
| CVE-2019-19499 Grafana Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | |
| Grafana 6.4.3 Arbitrary File Read – PT SWARM | MISC | swarm.ptsecurity.com | Exploit, Third P |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, anal |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[940011](#) AlmaLinux Security Update for grafana (ALSA-2020:4682)

[997821](#) GO (Go) Security Update for github.com/grafana/grafana/pkg/tsdb/mysql (GHSA-4pwp-cx67-5cpx)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)