



CVE-2022-38790

Published on: Not Yet Published

Last Modified on: 09/07/2022 05:06:00 PM UTC

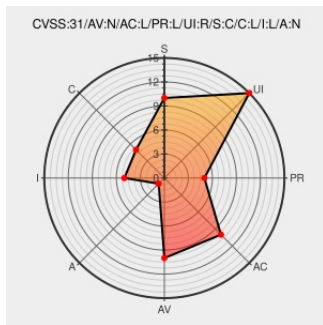
CVE-2022-38790

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Gitops](#) from [Weave.works](#) contain the following vulnerability:

Weave GitOps Enterprise before 0.9.0-rc.5 has a cross-site scripting (XSS) bug allowing a malicious user to inject a javascript: link in the UI. When clicked by a victim user, the script will execute with the victim's permission. The exposure appears in Weave GitOps Enterprise UI via a GitopsCluster dashboard link. An annotation can be added to a

GitopsCluster custom resource.

CVE-2022-38790 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|----------------|------------------------|---------------------|---------------------|
| NETWORK | LOW | LOW | REQUIRED |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| CHANGED | LOW | LOW | NONE |

CVE References

| Description | Tags | Link |
|--|--|---|
| Weave GitOps Enterprise - GitOps at Scale Weaveworks | www.weave.works text/html | www.weave.works/product/gitops-enterprise/ |
| Malicious links can be crafted by users and shown in the UI Weave GitOps | docs.gitops.weave.works text/html | docs.gitops.weave.works/security/cve/enterprise/CVE-2022-38790/index.html |
| Introduction Weave GitOps | docs.gitops.weave.works text/html | docs.gitops.weave.works/docs/intro |
| Getting started Weave GitOps | docs.gitops.weave.works text/html | docs.gitops.weave.works/docs/cluster-management/getting-started/#profiles-and-clusters |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport's website. We have provided these links to other resources because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------------------------|------------------------|---------|--------|---------|----------|
| Application | Weave.works | Gitops | All | All | All | All |
| Application | Weave.works | Gitops | 0.9.0 | rc1 | All | All |
| Application | Weave.works | Gitops | 0.9.0 | rc2 | All | All |
| Application | Weave.works | Gitops | 0.9.0 | rc3 | All | All |

cpe:2.3:a:weave.works:gitops:*:*:*:enterprise:*:*:




cpe:2.3:a:weave.works:gitops:0.9.0:rc1:*:*:enterprise:*:*:

cpe:2.3:a:weave.works:gitops:0.9.0:rc2:*:*:enterprise:*:*:

cpe:2.3:a:weave.works:gitops:0.9.0:rc3:*:*:enterprise:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|--|--|------------------------|
|  @CVEreport | CVE-2022-38790 : Weave GitOps Enterprise before 0.9.0-rc.5 has a cross-site scripting #XSS bug allowing a malicio... twitter.com/i/web/status/1... | 2022-09-01 13:02:20 |
|  @Inceptus3 | New Vulnerability: CVE-2022-38790 #InceptusSecure #UnderOurProtection | 2022-09-01 14:21:52 |
|  /r/netcve | CVE-2022-38790 | 2022-09-01 13:39:13 |

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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