Malicious links can be crafted by users and shown in the UI

Impact

Unpatched versions of Weave GitOps Enterprise are vulnerable to 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.

```
apiVersion: gitops.weave.works/v1alpha1
kind: GitopsCluster
metadata:
  name: demo-02
  namespace: default
  annotations:
    metadata.weave.works/dashboard.hellothere: "javascript:alert('hello there ' +
window.localStorage.getItem('name'));"
```

The attacker does not need access to the Weave GitOps UI to craft an attack. It could be crafted by modifying the resources via Git repository or Kubernetes API.

Patches

v0.9.0-rc.5

Workarounds

Given that the exposure comes from modifications done in `GitopsCluster` objects, the mitigation comes around establishing the controls to avoid that an attacker could modify them.

1. Via Git, by ensuring that no modifications to `GitopsCluster` are done without review or control that avoids it.
2. Via Kubernetes API, by ensuring that access to `GitopsCluster` resources is properly protected via RBAC.

References

- https://docs.gitops.weave.works/docs/next/cluster-management/getting-started/#profiles-and-clusters
- CVE-2022-38790

For more information

If you have any questions or comments about this advisory:

- Email us at security@weave.works