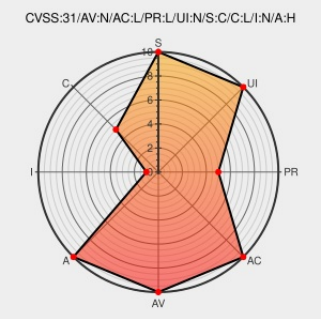
CVE-2021-32783

Published on: 07/23/2021 12:00:00 AM UTC

Last Modified on: 08/05/2021 04:56:00 PM UTC

CVE-2021-32783 - advisory for GHSA-5ph6-qq5x-7jwc

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Contour from Projectcontour contain the following vulnerability:

Contour is a Kubernetes ingress controller using Envoy proxy. In Contour before version 1.17.1 a specially crafted ExternalName type Service may be used to access Envoy's admin interface, which Contour normally prevents from access outside the Envoy container. This can be used to shut down Envoy remotely (a denial of service), or to expose the existence of any Secret that Envoy is using for its configuration, including most notably TLS Keypairs. However, it *cannot* be used to get the *content* of those secrets. Since this attack allows access to the administration interface, a variety of administration options are available, such as shutting down the Envoy or draining traffic. In general, the Envoy admin interface cannot easily be used for making changes to the cluster, in-flight requests, or backend services, but it could be used to shut down or drain Envoy, change traffic routing, or to retrieve secret metadata, as mentioned above. The issue will be addressed in Contour v1.18.0 and a cherry-picked patch release, v1.17.1, has been released to cover users who cannot upgrade at this time. For more details refer to the linked GitHub Security Advisory.

CVE-2021-32783 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **projectcontour** - **contour** version **< 1.17.1**

CVSS3 Score: 8.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	NONE	HIGH

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
ExternalName Services can be used to gain access to Envoy's admin interface · Advisory · projectcontour/contour · GitHub	github.com text/html	CONFIRM github.com/projectcontour/contour/security/advisories/GHSA-5ph6-qq5x-7jwc
Release Contour v1.17.1 · projectcontour/contour · GitHub	github.com text/html	MISC github.com/projectcontour/contour/releases/tag/v1.17.1
cherrypicks for v1.17.1 (#3909) · projectcontour/contour@b53a5c4 · GitHub	github.com text/html	MISC github.com/projectcontour/contour/commit/b53a5c4fd927f4ea2c6cf02f1359d8e28bef852e

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Projectcontour	Contour	All	All	All	All

cpe:2.3:a:projectcontour:contour:*:*:*:*:*:kubernetes:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32783 : Contour is a Kubernetes ingress controller using Envoy proxy. In Contour before version 1.17.1 a s… twitter.com/i/web/status/1…	2021-07-23 21:55:46
@LinInfoSec	Kubernetes - CVE-2021-32783: github.com/projectcontour…	2021-07-24 01:20:32
/r/netcve	CVE-2021-32783	2021-07-23 22:38:28

← Previous ID

Next ID→

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