



CVE-2020-8660

Published on: 03/04/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8660

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Envoy](#) from [Envoyproxy](#) contain the following vulnerability:

CNCF Envoy through 1.13.0 TLS inspector bypass. TLS inspector could have been bypassed (not recognized as a TLS client) by a client using only TLS 1.3. Because TLS extensions (SNI, ALPN) were not inspected, those connections might have been matched to a wrong filter chain, possibly bypassing some security restrictions in the

process.

CVE-2020-8660 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
TLS inspector bypass · Advisory · envoyproxy/envoy · GitHub	Third Party Advisory github.com	MISC github.com/envoyproxy/envoy/security/advisories/GHSA-c4g8-

text/html

7grc-5wvx

Version history — envoy tag-v1.13.1 documentation

Vendor Advisory

www.envoyproxy.io

text/html

CONFIRM

www.envoyproxy.io/docs/envoy/v1.13.1/intro/version_history

Red Hat Customer Portal

Third Party Advisory

access.redhat.com

text/html

REDHAT RHSA-2020:0734

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites 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	Envoyproxy	Envoy	All	All	All	All
Application	Envoyproxy	Envoy	All	All	All	All

cpe:2.3:a:envoyproxy:envoy:*****:*

cpe:2.3:a:envoyproxy:envoy:*****:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→