



CVE-2020-15104

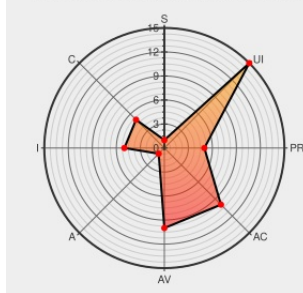
Published on: 07/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-15104 - advisory for GHSA-w5f5-6qh-q-hhrg

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

CVSS:31/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N



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

In Envoy before versions 1.12.6, 1.13.4, 1.14.4, and 1.15.0 when validating TLS certificates, Envoy would incorrectly allow a wildcard DNS Subject Alternative Name apply to multiple subdomains. For example, with a SAN of *.example.com, Envoy would incorrectly allow nested.subdomain.example.com, when it should only allow

subdomain.example.com. This defect applies to both validating a client TLS certificate in mTLS, and validating a server TLS certificate for upstream connections. This vulnerability is only applicable to situations where an untrusted entity can obtain a signed wildcard TLS certificate for a domain of which you only intend to trust a subdomain of. For example, if you intend to trust api.mysubdomain.example.com, and an untrusted actor can obtain a signed TLS certificate for *.example.com or *.com. Configurations are vulnerable if they use verify_subject_alt_name in any Envoy version, or if they use match_subject_alt_names in version 1.14 or later. This issue has been fixed in Envoy versions 1.12.6, 1.13.4, 1.14.4, 1.15.0.

CVE-2020-15104 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: envoyproxy - envoy version < 1.12.6

Affected Vendor/Software: envoyproxy - envoy version >= 1.13.0, < 1.13.4

Affected Vendor/Software: envoyproxy - envoy version >= 1.14.0, < 1.14.4

CVSS3 Score: **5.4 - MEDIUM**

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

UNCHANGED

LOW

LOW

NONE

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
TLS cert wildcard · Advisory · envoyproxy/envoy · GitHub	Third Party Advisorygithub.comtext/html	CONFIRMgithub.com/envoyproxy/envoy/security/advisories/GHSA-w5f5-6qhq-hhrg

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 →