

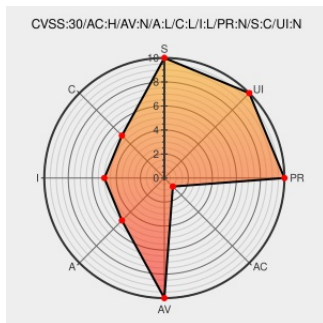


CVE-2019-9901

Published on: 04/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2019-9901

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

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

Envoy 1.9.0 and before does not normalize HTTP URL paths. A remote attacker may craft a relative path, e.g., something/../admin, to bypass access control, e.g., a block on /admin. A backend server could then interpret the non-normalized path and provide an attacker access beyond the scope provided for by the access control policy.

CVE-2019-9901 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **10 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Version history — envoy tag-v1.9.1 documentation	Release Notes Vendor Advisory www.envoyproxy.io	CONFIRM www.envoyproxy.io/docs/envoy/v1.9.1/intro/version_history

	text/html	
Google Groups	Patch Third Party Advisory groups.google.com text/html	CONFIRM groups.google.com/forum/#!topic/envoy-announce/VoHfnDqZiAM
Missing HTTP URL path normalization · Advisory · envoyproxy/envoy · GitHub	github.com text/html	CONFIRM github.com/envoyproxy/envoy/security/advisories/GHSA-xcx5-93pw-jw2w
CVE-2019-9901 · Issue #6435 · envoyproxy/envoy · GitHub	Issue Tracking Mitigation Third Party Advisory github.com text/html	CONFIRM github.com/envoyproxy/envoy/issues/6435

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →