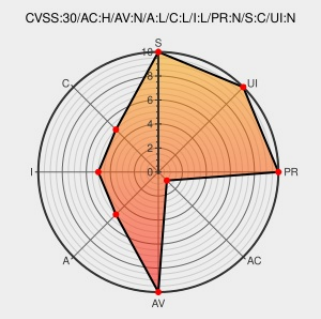
CVE-2019-9900

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

Last Modified on: 11/07/2023 03:13:00 AM UTC

CVE-2019-9900

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Envoy from Envoyproxy contain the following vulnerability:

When parsing HTTP/1.x header values, Envoy 1.9.0 and before does not reject embedded zero characters (NUL, ASCII 0x0). This allows remote attackers crafting header values containing embedded NUL characters to potentially bypass header matching rules, gaining access to unauthorized resources.

CVE-2019-9900 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.3 - HIGH

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

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	
NUL characters in HTTP/1 headers allow access control bypass (CVE-2019-9900) · Advisory · envoyproxy/envoy · GitHub	github.com text/html	CONFIRM github.com/envoyproxy/envoy/security/advisories/GHSA-x74r-f4mw-c32h
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2019:0741
Google Groups	groups.google.com text/html	CONFIRM groups.google.com/forum/#!topic/envoy-announce/VoHfnDqZiAM
CVE-2019-9900 · Issue #6434 · envoyproxy/envoy · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	CONFIRM github.com/envoyproxy/envoy/issues/6434

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	Redhat	Openshift Service Mesh	-	All	All	All

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

cpe:2.3:a:redhat:openshift_service_mesh:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→