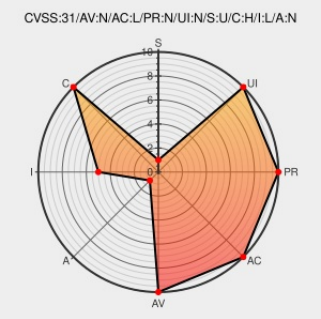
CVE-2021-21378

Published on: 03/10/2021 12:00:00 AM UTC

Last Modified on: 10/24/2022 05:11:00 PM UTC

CVE-2021-21378 - advisory for GHSA-4996-m8hf-hj27

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



Certain versions of Envoy from Envoyproxy contain the following vulnerability:

Envoy is a cloud-native high-performance edge/middle/service proxy. In Envoy version 1.17.0 an attacker can bypass authentication by presenting a JWT token with an issuer that is not in the provider list when Envoy's JWT Authentication filter is configured with the `allow_missing` requirement under `requires_any` due to a mistake in implementation. Envoy's JWT Authentication filter can be configured with the `allow_missing` requirement that will be satisfied if JWT is missing (JwtMissed error) and fail if JWT is presented or invalid. Due to a mistake in implementation, a JwtUnknownIssuer error was mistakenly converted to JwtMissed when `requires_any` was configured. So if `allow_missing` was configured under `requires_any`, an attacker can bypass authentication by presenting a JWT token with an issuer that is not in the provider list. Integrity may be impacted depending on configuration if the JWT token is used to protect against writes or modifications. This regression was introduced on 2020/11/12 in PR 13839 which fixed handling `allow_missing` under RequiresAny in a JwtRequirement (see issue 13458). The AnyVerifier aggregates the children verifiers' results into a final status where JwtMissing is the default error. However, a JwtUnknownIssuer was mistakenly treated the same as a JwtMissing error and the resulting final aggregation was the default JwtMissing. As a result, `allow_missing` would allow a JWT token with an unknown issuer status. This is fixed in version 1.17.1 by PR 15194. The fix works by preferring JwtUnknownIssuer over a JwtMissing error, fixing the accidental conversion and bypass with `allow_missing`. A user could detect whether a bypass occurred if they have Envoy logs enabled with debug verbosity. Users can enable component level debug logs for JWT. The JWT filter logs will indicate that there is a request with a JWT token and a failure that the JWT token is missing.

CVE-2021-21378 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **envoyproxy** - **envoy** version **= 1.17.0**

CVSS3 Score: 8.2 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
jwt_authn: fix a bug where JWT with wrong issuer is allowed in allow_… · envoyproxy/envoy@ea39e3c · GitHub	github.com text/html	MISC github.com/envoyproxy/envoy/commit/ea39e3cba652bcc4b11bb0d5c62b017e584d2e5a
jwt_authn: fix a bug where JWT with wrong issuer is allowed in allow_missing case by qiwzhang · Pull Request #15194 · envoyproxy/envoy · GitHub	github.com text/html	MISC github.com/envoyproxy/envoy/pull/15194
JWT authentication bypass with unknown issuer token · Advisory · envoyproxy/envoy · GitHub	github.com text/html	CONFIRM github.com/envoyproxy/envoy/security/advisories/GHSA-4996-m8hf-hj27

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	1.17.0	All	All	All

cpe:2.3:a:envoyproxy:envoy:1.17.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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