Bypass of RBAC uri_template permission

Moderate **phlax** published **GHSA-c7cm-838g-6g67** 20 hours ago

Package	Affected versions	Patched versions
No package listed	<v1.34.1, <v1.33.3, <v1.32.6, <v1.31.8	v1.34.1, v1.33.3, v1.32.6, v1.31.8

Description

Summary

Envoy's URI template matcher does not match URI paths containing the `*` character.

Affected Components

Envoy's URI template matcher and Envoy's HTTP RBAC extension when configured with the `uri_template` permissions.

Details

Envoy's URI template matcher incorrectly excludes the `*` character from a set of valid characters in the URI path. As a result URI path containing the `*` character will not match a URI template expressions.

Impact

Bypass of RBAC rules when configured using the `uri_template` permissions.

Attack vector(s)

A request from an untrusted peer with URI path containing the `*` character.

Patches

This vulnerability is fixed in Envoy versions v1.34.1, v1.33.3, v1.32.6, v1.31.8

Workarounds

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE ID

CVE-2025-46821

Weaknesses

CWE-186

Credits

yanavlasov	Remediation reviewe
botengyao	Coordinator
phlax	Coordinator
barchw	Reporter

Configure additional RBAC permissions using `url_path` with `safe_regex` expression.

Detection

Access log entries to excluded endpoints with the `*` character(s) in request URI path.

Credits

Discovery: "Chwila, Bartosz" bartosz.chwila@sap.com
Diagnostics: Jackie Maertens (Elliott): https://github.com/jaellio