Kyverno is vulnerable to server-side request forgery (SSRF)

Vulnerability Note VU#655822

Original Release Date: 2026-03-30 | Last Revised: 2026-03-30

Overview

Kyverno, versions 1.16.0 to present, contains an SSRF vulnerability in its CEL-based HTTP functions, which lack URL validation or namespace scoping and allow namespaced policies to trigger arbitrary internal HTTP requests. An attacker with only namespace-level permissions can exploit this to access sensitive internal services via the highly privileged Kyverno admission controller.

Description

Kyverno is an open-source, Kubernetes-native policy engine that functions as a dynamic admission controller for the Kubernetes API. It is designed to manage the lifecycle of cluster resources by validating, mutating, and generating configurations based on YAML-defined policies. Within a security context, the engine is frequently utilized to enforce Pod Security Standards, verify image signatures via Cosign, and audit resource configurations for compliance. Because Kyverno

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

operates with high-level permissions to intercept and modify API requests, it represents a critical component of the cluster's security posture and trust boundary.

A server-side request forgery vulnerability exists in Kyverno's CEL-based HTTP functions (Get and Post) used by namespaced policy types in the `policies.kyverno.io` API group. Unlike Kyverno's resource library, which enforces namespace boundaries, the HTTP library at `pkg/cel/libs/http/http.go` performs no URL validation or scoping; i.e., there are no blocklists, namespace restrictions, or destination checks. As a result, these policies can issue arbitrary HTTP requests from the Kyverno admission controller pod.

Impact

An authenticated attacker with only namespace-scoped permissions can create a malicious namespaced policy that sends an internal `http.Get()` request, captures the response in a CEL variable, and exfiltrates it via the policy's `messageExpression` field returned in the admission denial. Because requests originate from the Kyverno admission controller, which often has privileged network reachability across internal cluster services and cloud metadata APIs, this enables cross-namespace data access and potential exposure of sensitive metadata or service responses, effectively breaking Kyverno's intended security boundaries through SSRF.

Solution

Unfortunately, we were unable to reach the vendor to coordinate this vulnerability. Since a patch is unavailable, we can only offer mitigation strategies.

Mitigation should include implementing strict URL validation and destination controls within Kyverno's CEL HTTP library to ensure parity with the namespace-scoped restrictions enforced by the resource library. Recommended safeguards include blocking access to link-local and cloud metadata address ranges, limiting outbound requests to approved in-cluster services, and providing administrators with configurable allowlists. Additionally, applying default deny network

policies to the Kyverno admission controller pod can reduce residual risk by preventing unauthorized egress in the event of future validation gaps.

Acknowledgements

Thanks to Igor Stepansky from Orca Security Research Pod for responsibly disclosing this vulnerability. This document was written by Dr. Elke Drennan, CISSP.

Vendor Information

Filter by status: All

Filter by content:

Additional information available

Sort by: Status

Expand all

Kyverno	Unknown

References

- **https://github.com/kyverno/kyverno**
- **https://portswigger.net/web-security/ssrf**
- **https://github.com/kyverno/kyverno/pull/15729**

Other Information

CVE IDs:	CVE-2026-4789
API URL:	VINCE JSON | CSAF
Date Public:	2026-03-30
Date First Published:	2026-03-30
Date Last Updated:	2026-03-30 18:19 UTC
Document Revision:	3

Sponsored by CISA.

Download PGP Key

Read CERT/CC Blog

Learn about Vulnerability Analysis

Carnegie Mellon University
Software Engineering
Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact SEI

Contact CERT/CC

412-268-5800
cert@cert.org