ISTIO-SECURITY-2021-005

HTTP request paths with multiple slashes or escaped slash characters may bypass path based authorization rules.

May 11, 2021

Disclosure Details	
CVE(s)	CVE-2021-31920
CVSS Impact Score	8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Affected Releases	All releases prior to 1.8.6 1.9.0 to 1.9.4

Issue

Istio contains a remotely exploitable vulnerability where an HTTP request path with multiple slashes or escaped slash characters (`%2F` or `%5C`) could potentially bypass an Istio authorization policy when path based authorization rules are used. Related Envoy CVE: `CVE-2021-29492`.

For example, assume an Istio cluster administrator defines an authorization DENY policy to reject the request at path `/admin`. A request sent to the URL path `//admin` will NOT be rejected by the authorization policy.

According to the RFC 3986, the path `//admin` with multiple slashes should technically be treated as a different path from the `/admin`. However, some backend services choose to normalize the URL paths by merging multiple slashes to a single slash. This can result in a bypass of the authorization policy (`//admin` does not match `/admin`) and a user can access the resource at path `/admin` in the backend; this would represent a security incident.

Am I impacted?

Your cluster is **impacted** by this vulnerability if you have authorization policies using `ALLOW action + notPaths field` or `DENY action + paths field` patterns. These patterns are vulnerable to unexpected policy bypasses and you should upgrade to fix the security issue as soon as possible.

The following is an example of vulnerable policy that uses `DENY action + paths field` pattern:

```
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
metadata:
name: deny-path-admin
spec:
action: DENY
rules:
- to:
    - operation:
        paths: ["/admin"]
```

The following is another example of vulnerable policy that uses `ALLOW action + notPaths field` pattern:

```
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
metadata:
name: allow-path-not-admin
spec:
action: ALLOW
rules:
- to:
    - operation:
        notPaths: ["/admin"]
```

Your cluster is **NOT impacted** by this vulnerability if:

- You don't have authorization policies
- Your authorization policies don't define `paths` or `notPaths` fields.
- Your authorization policies use `ALLOW action + paths field` or `DENY action + notPaths field` patterns. These patterns could only cause unexpected rejection instead of policy bypasses. The upgrade is optional for these cases.

Mitigation

1. Update your cluster to the latest supported version. These versions support configuring the Envoy proxies in the system with more normalization options:

- Istio 1.8.6, if using 1.8.x
- Istio 1.9.5 or up
- The patch version specified by your cloud provider

1. Follow the security best practices to configure your authorization policies.

Credit

We would like to thank `Ruilin` and `Test123` for discovering this issue.