ISTIO-SECURITY-2021-006

An external client can access unexpected services in the cluster, bypassing authorization checks, when a gateway is configured with AUTO_PASSTHROUGH routing configuration.

May 11, 2021

Disclosure Details	
CVE(s)	CVE-2021-31921
CVSS Impact Score	10 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
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 external client can access unexpected services in the cluster, bypassing authorization checks, when a gateway is configured with `AUTO_PASSTHROUGH` routing configuration.

Am I impacted?

This vulnerability impacts only usage of the `AUTO_PASSTHROUGH` Gateway type, which is typically only used in multi-network multi-cluster deployments.

The TLS mode of all Gateways in the cluster can be detected with the following command:

```
$ kubectl get gateways.networking.istio.io -A -o "custom-columns=NAMESPACE:.metadata.namespace,NAME:.metadata.name,TLS_MODE:.spec.servers[*].tls.mode"
```

If the output shows any `AUTO_PASSTHROUGH` Gateways, you may be impacted.

Mitigation

Update your cluster to the latest supported version:

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

Credit

We would like to thank John Howard (Google) for reporting this issue.