ISTIO-SECURITY-2020-009

Incorrect Envoy configuration for wildcard suffixes used for Principals/Namespaces in Authorization Policies for TCP Services.

Aug 11, 2020

Disclosure Details	
CVE(s)	CVE-2020-16844
CVSS Impact Score	6.8 AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N
Affected Releases	1.5 to 1.5.8 1.6 to 1.6.7

Istio is vulnerable to a newly discovered vulnerability:

- `CVE-2020-16844`: Callers to TCP services that have a defined Authorization Policies with `DENY` actions using wildcard suffixes (e.g. `*-some-suffix`) for source principals or namespace fields will never be denied access.
  - CVSS Score: 6.8 AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

Istio users are exposed to this vulnerability in the following ways:

If the user has an Authorization similar to

```
apiVersion: security.istio.io/v1beta1
kind: AuthorizationPolicy
metadata:
 name: foo
 namespace: foo
spec:
 action: DENY
 rules:
 - from:
   - source:
       principals:
       - */ns/ns1/sa/foo # indicating any trust domain, ns1 namespace, foo svc account
```

Istio translates the principal (and `source.principal`) field to an Envoy level string match

```
stringMatch:
  suffix: spiffe:///ns/ns1/sa/foo
```

which will not match any legitimate caller as it included the `spiffe://` string incorrectly. The correct string match should be

```
stringMatch:
  regex: spiffe://.*/ns/ns1/sa/foo
```

Prefix and exact matches in `AuthorizationPolicy` is unaffected, as are ALLOW actions in them; HTTP is also unaffected.

Mitigation

- For Istio 1.5.x deployments: update to Istio 1.5.9 or later.
- For Istio 1.6.x deployments: update to Istio 1.6.8 or later.
- Do not use suffix matching in DENY policies in the source principal or namespace field for TCP services and use Prefix and Exact matching where applicable. Where possible change TCP to HTTP for port name suffixes in your Services.

Reporting vulnerabilities

We'd like to remind our community to follow the vulnerability reporting process to report any bug that can result in a security vulnerability.