# CVE Detail – CVE-2021-39155

Istio is an open source platform for providing a uniform way to integrate microservices, manage traffic flow across microservices, enforce policies and aggregate telemetry data. According to [RFC 4343](https://datatracker.ietf.org/doc/html/rfc4343), Istio authorization policy should compare the hostname in the HTTP Host header in a case insensitive way, but currently the comparison is case sensitive. The proxy will route the request hostname in a case-insensitive way which means the authorization policy could be bypassed. As an example, the user may have an authorization policy that rejects request with hostname "httpbin.foo" for some source IPs, but the attacker can bypass this by sending the request with hostname "Httpbin.Foo". Patches are available in Istio 1.11.1, Istio 1.10.4 and Istio 1.9.8. As a work around a Lua filter may be written to normalize Host header before the authorization check. This is similar to the Path normalization presented in the [Security Best Practices](https://istio.io/latest/docs/ops/best-practices/security/#case-normalization) guide.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.43815

## CVSS Scoring

CVSS v3.1 Score: 8.3

Severity: HIGH

## Mapped CWE(s)

* CWE-178: Improper Handling of Case Sensitivity
* CWE-863: Incorrect Authorization

## Affected Products

* cpe:2.3:a:istio:istio:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:istio:istio:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:istio:istio:\*:\*:\*:\*:\*:\*:\*:\*