# CVE Detail – CVE-2022-24766

mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.4 and below, a malicious client or server is able to perform HTTP request smuggling attacks through mitmproxy. This means that a malicious client/server could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. While mitmproxy would only see one request, the target server would see multiple requests. A smuggled request is still captured as part of another request's body, but it does not appear in the request list and does not go through the usual mitmproxy event hooks, where users may have implemented custom access control checks or input sanitization. Unless mitmproxy is used to protect an HTTP/1 service, no action is required. The vulnerability has been fixed in mitmproxy 8.0.0 and above. There are currently no known workarounds.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.70344

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

## CAPEC(s)

* CAPEC-273: HTTP Response Smuggling
* CAPEC-33: HTTP Request Smuggling

## Affected Products

* cpe:2.3:a:mitmproxy:mitmproxy:\*:\*:\*:\*:\*:\*:\*:\*