



CVE-2023-37276

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-37276
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-19 20:15:00 UTC
Updated	2023-07-28 15:55:00 UTC
Description	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. aiohttp v3.8.4 and earlier are bundled with

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aiohttp Project	Aiohttp	All	All	All	All

References

Reference	Source
HackerOne	MISC
github.com/aio-lib/aiohttp/blob/v3.8.4/.gitmodules	MISC
aiohttp.web.Application vulnerable to HTTP request smuggling via llhttp HTTP request parser · Advisory · aio-lib/aiohttp · GitHub	MISC
Fix bump llhttp to v8.1.1 (#7367) (#7377) · aio-lib/aiohttp@9337fb3 · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)