CVE-2023-37276

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

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 wit

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

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report