



CVE-2023-26151

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-26151
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-03 05:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Versions of the package asyncua before 0.9.96 are vulnerable to Denial of Service (DoS) such that an attacker can send a

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freeopcua	Opcua-asyncio	All	All	All	All

References

Reference	Source	Link	Tags
Release v0.9.96 · FreeOpcUa/opcua-asyncio · GitHub	MISC	github.com	
server handle malformed packets by oroulet · Pull Request #1039 · FreeOpcUa/opcua-asyncio · GitHub	MISC	github.com	
DoS asyncua Server · GitHub	MISC	gist.github.com	
Denial of Service (DoS) in asyncua CVE-2023-26151 Snyk	MISC	security.snyk.io	
Denial of Service · Issue #1013 · FreeOpcUa/opcua-asyncio · GitHub	MISC	github.com	
server handle malformed packets · FreeOpcUa/opcua-asyncio@f6603da · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995510](#) Python (Pip) Security Update for asyncua (GHSA-gfvq-mxw3-mfq3)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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