CVE-2023-26150

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

Summary

CVE	CVE-2023-26150
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 Improper Authentication such that it is possible to access

Risk And Classification

Problem Types: CWE-287

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	Ta
Release v0.9.96 · FreeOpcUa/opcua-asyncio · GitHub	MISC	github.com	
check if session is activated by schroeder- · Pull Request #1015 · FreeOpcUa/opcua-asyncio · GitHub	MISC	github.com	
check if session is active · FreeOpcUa/opcua-asyncio@b4106df · GitHub	MISC	github.com	
Improper Authentication in asyncua | CVE-2023-26150 | Snyk	MISC	security.snyk.io	
Illegal access to Address Space · Issue #1014 · FreeOpcUa/opcua-asyncio · GitHub	MISC	github.com	
illegal access to address space · GitHub	MISC	gist.github.com	
Revert "releax test_secure_channel_key_expiration test" · FreeOpcUa/opcua-asyncio@2be7ce8 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995509 Python (Pip) Security Update for asyncua (GHSA-2894-qcqf-g23g)