



Out-of-bounds write in Windows asyncio.ProactorEventLoop.sock_recvfrom_into() when using nbytes

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2026-3298
State	PUBLISHED
Assigner	PSF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 15:16:37 UTC
Updated	2026-04-21 21:16:41 UTC
Description	The method "sock_recvfrom_into()" of "asyncio.ProactorEventLoop" (Windows only) was missing a boundary check for the

Risk And Classification

Primary CVSS: v4.0 8.8 HIGH from cna@python.org

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000500000 probability, percentile 0.156450000 (date 2026-04-22)

Problem Types: CWE-787 | CWE-787 CWE-787 Out-of-bounds write

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	

None

Confidentiality

Low

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

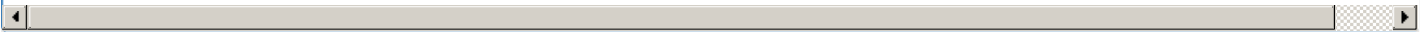


Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Python Software Foundation	CPython	affected 3.11.0 3.15.0 python	Not specified

References

Reference	Source	Link	Tags
github.com/python/cpython/commit/95633d2aad4721e25e4dfd9f43dfb6e1edcbd741	cna@python.org	github.com	
github.com/python/cpython/pull/148809	cna@python.org	github.com	
github.com/python/cpython/issues/148808	cna@python.org	github.com	
github.com/python/cpython/commit/27522b7d6e6588f03e61099dd858cd5a9314e2f2	cna@python.org	github.com	
mail.python.org/archives/list/security-announce@python.org/thread/KWTPIQBOOOU...	cna@python.org	mail.python.org	
github.com/python/cpython/commit/1274766d3c29007ab77245a72abbf8dce2a9db4d	cna@python.org	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal



Vendor Comments And Credit

Discovery Credit

CNA: GGAutomaton (https://github.com/GGAutomaton) (en)

CNA: Victor Stinner (https://github.com/vstinner) (en)

CNA: Seth Larson (https://github.com/sethmlarson) (en)

There are currently no legacy CID mappings associated with this CVE

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

© [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](#).

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

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