



CVE-2020-29396

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

Summary

CVE	CVE-2020-29396
State	PUBLIC
Assigner	security@odoo.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-22 17:15:00 UTC
Updated	2023-02-02 22:21:00 UTC
Description	A sandboxing issue in Odoo Community 11.0 through 13.0 and Odoo Enterprise 11.0 through 13.0, when running with Pyth

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Odoo	Odoo	All	All	All	All
Application	Odoo	Odoo	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All

References

Reference	Source	Link
[SEC] CVE-2020-29396 - Affects: Odoo 11.0 through 14.0 (Community a... · Issue #63712 · odoo/odoo · GitHub	MISC	github.com
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.cc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Toufik Ben Jaa

LEGACY: Stéphane Debauche

LEGACY: Benoît FONTAINE

Legacy QID Mappings

900046 CBL-Mariner Linux Security Update for python3 3.7.9

902871 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (3706)

© [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](#)