



CVE-2023-36814

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

Summary

CVE	CVE-2023-36814
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-03 17:15:00 UTC
Updated	2023-07-17 18:56:00 UTC
Description	Products.CMFCore are the key framework services for the Zope Content Management Framework (CMF). The use of Python's marshal module is not checked for untrusted input, which can lead to a denial of service or a crash via unchecked use of input with Python's marshal module.

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zope	Products.cmfcore	All	All	All	All

References

Reference

- Merge pull request from GHSA-4hpj-8rhv-9x87 · zopefoundation/Products.CMFCore@40f03f4 · GitHub
- Unauthenticated denial of service and crash via unchecked use of input with Python's marshal module · Advisory · zopefoundation/Products.CMFCore
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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