



CVE-2024-22362

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2024-22362
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-16 04:15:00 UTC
Updated	2024-01-23 18:18:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	9.3.6	-	All	All

References

Reference

- [Drupal core release schedule | Core release cycles | About guide on Drupal.org](#)
- [GitHub - drupal/drupal: Verbatim mirror of the git.drupal.org repository for Drupal core. Please see the https://github.com/drupal/drupal#contrib](#)
- [Drupal - Open Source CMS | Drupal.org](#)
- [JVN#63383723: Drupal vulnerable to improper handling of structural elements](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [154147](#) Drupal Denial of Service (DoS) Vulnerability (CVE-2024-22362)
- [996764](#) PHP (Composer) Security Update for drupal/core (GHSA-62cf-jvpp-48q6)

© [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](#)