



CVE-2023-51467

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

Summary

CVE	CVE-2023-51467
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-26 15:15:00 UTC
Updated	2024-01-04 09:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ofbiz	All	All	All	All

References

Reference	Source	Link
ofbiz.apache.org/security.html		ofbiz.apache.c
lists.apache.org/thread/oj2s6objhdq72t6g29omqpcbd1wlp48o		lists.apache.or
oss-security - CVE-2023-51467: Apache OFBiz: Pre-authentication Remote Code Execution (RCE) vulnerability		www.openwall
ofbiz.apache.org/download.html		ofbiz.apache.c
lists.apache.org/thread/9tmf9qyyhgh6m052rhz7lg9vxn390bdv		lists.apache.or
issues.apache.org/jira/browse/OFBIZ-12873		issues.apache
ofbiz.apache.org/release-notes-18.12.11.html		ofbiz.apache.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150768](#) Apache OFBiz: Pre-Auth Remote Code Execution Vulnerability (CVE-2023-51467)

[731049](#) Apache OFBiz Authentication Bypass Vulnerability

© [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](#)