



CVE-2024-23525

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

Summary

CVE	CVE-2024-23525
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-18 00:15:00 UTC
Updated	2024-01-27 22:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tozt	Spreadsheet	\	parsexlsx	All	All

References

Reference	Source	Link
metacpan.org/release/NUDDLEGG/Spreadsheet-ParseXLSX-0.30/changes		metacpan.org
github.com/MichaelDaum/spreadsheet-parsexlsx/issues/10		github.com
[debian-lts-announce] 20240127 [SECURITY] [DLA 3723-1] libspreadsheet-parsexlsx-perl security update		lists.debian.org
[oss-security] 20240118 CVE-2024-23525: Spreadsheet::ParseXLSX for Perl is vulnerable to XXE attacks		www.openwall.com
gist.github.com/phvietan/d1c95a88ab6e17047b0248d6bf9eac4a		gist.github.com
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

6000451 Debian Security Update for libspreadsheet-parsexlsx-perl (DLA 3723-1)

© [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](#)