



CVE-2021-31598

Published on: 04/24/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 04:04:00 PM UTC

CVE-2021-31598

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode() performs incorrect memory handling while parsing crafted XML files, leading to a heap-based buffer overflow.

CVE-2021-31598 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 2705-1] scilab security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210708 [SECURITY] [DLA 2705-1] scilab security update
ezXML / Bugs / #28 Out-of-bounds write in ezxml_decode() leading to heap corruption	sourceforge.net text/html	MISC sourceforge.net/p/ezxml/bugs/28/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[178700](#) Debian Security Update for scilab (DLA 2705-1)

[182899](#) Debian Security Update for netcdfnetcdf-parallel (CVE-2021-31598)

[751404](#) OpenSUSE Security Update for netcdf (openSUSE-SU-2021:3805-1)

[751405](#) OpenSUSE Security Update for netcdf (openSUSE-SU-2021:3804-1)

[751407](#) OpenSUSE Security Update for netcdf (openSUSE-SU-2021:1505-1)

[751409](#) OpenSUSE Security Update for netcdf (openSUSE-SU-2021:3815-1)

[751439](#) OpenSUSE Security Update for netcdf (openSUSE-SU-2021:3873-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Ezxml Project	Ezxml	0.8.6	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:ezxml_project:ezxml:0.8.6:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-31598 : An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode performs incorre... twitter.com/i/web/status/1...	2021-04-24 17:05:27

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)