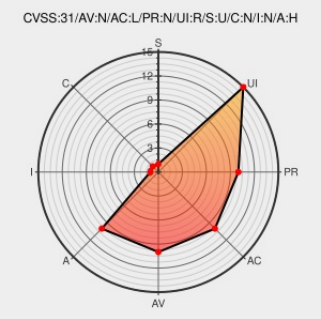
CVE-2021-31348

Published on: 04/16/2021 12:00:00 AM UTC

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

CVE-2021-31348

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_parse_str() performs incorrect memory handling while parsing crafted XML files (out-of-bounds read after a certain strcspn failure).

CVE-2021-31348 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
ezXML / Bugs / #27 Out-of-bounds read/write in ezxml_parse_str() in ezxml.c:586/587	sourceforge.net text/html	MISC sourceforge.net/p/ezxml/bugs/27/
[SECURITY] [DLA 2705-1] scilab security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210708 [SECURITY] [DLA 2705-1] scilab security update

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)

184765 Debian Security Update for netcdfnetcdf-parallel (CVE-2021-31348)

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.report/CVE-2021-31348 An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_parse_str perfo… twitter.com/i/web/status/1…	2021-04-16 20:35:36
@management_sun	IT Risk: SUSE.netcdfに複数の脆弱性 -1/2 サービス拒否状態にされる 機密データにアクセスされる セキュリティレベルが低下させられる CVE-2021-31598 CVE-2021-31348 CVE-202… twitter.com/i/web/status/1…	2021-11-29 08:18:52
@LinInfoSec	Debian - CVE-2021-31348: sourceforge.net/p/ezxml/bugs/2…	2022-04-19 06:19:42
/r/netcve	CVE-2021-31348	2021-04-16 20:57:06

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report