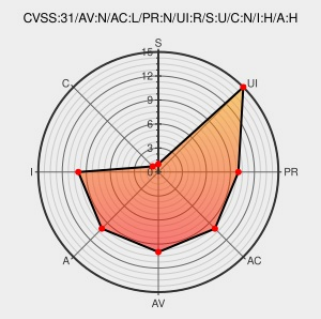
CVE-2021-26220

Published on: 02/08/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:29:02 PM UTC

CVE-2021-26220

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ezxml from Ezxml Project contain the following vulnerability:

The ezxml_toxml function in ezxml 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.

CVE-2021-26220 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
ezXML / Bugs / #23 Out-of-bounds write caused by incorrect error handling of malloc in ezxml_new (ezxml.c:750)	Exploit, Third Party Advisory, sourceforge.net, text/html	MISC sourceforge.net/p/ezxml/bugs/23/

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

182754 Debian Security Update for netcdfnetcdf-parallel (CVE-2021-26220)

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
Application	Ezxml Project	Ezxml	All	All	All	All

cpe:2.3:a:ezxml_project:ezxml:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@vigilance_fr	Vigil@nce #Vulnérabilité de ezXML : trois vulnérabilités. vigilance.fr/vulnerabilite/… Références : #CVE-2021-26220,… twitter.com/i/web/status/1…	2021-11-26 14:09:03
@vigilance_en	Vigil@nce #Vulnerability of ezXML: three vulnerabilities. vigilance.fr/vulnerability/… Identifiers: #CVE-2021-26220,… twitter.com/i/web/status/1…	2021-11-26 14:09:03
@management_sun	IT Risk: SUSE.netcdfに複数の脆弱性 -2/2 CVE-2021-26221 CVE-2021-26220 CVE-2019-20202 CVE-2019-20201 CVE-2019-20200 CVE-201… twitter.com/i/web/status/1…	2021-11-30 23:23:51
@management_sun	IT Risk: SUSE.Multiple vulnerabilities in netcdf -2/2 CVE-2021-26220 CVE-2019-20202 CVE-2019-20201 CVE-2019-20200 C… twitter.com/i/web/status/1…	2021-11-30 23:24:22
@management_sun	IT Risk: SUSE.netcdfに複数の脆弱性 -2/2 CVE-2021-26222 CVE-2021-26221 CVE-2021-26220 CVE-2019-20202 CVE-2019-20201 CVE-201… twitter.com/i/web/status/1…	2021-12-03 01:27:01
@management_sun	IT Risk: SUSE.Multiple vulnerabilities in netcdf -2/2 CVE-2021-26220 CVE-2019-20202 CVE-2019-20201 CVE-2019-20200 C… twitter.com/i/web/status/1…	2021-12-03 01:27:36

← Previous ID Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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