



CVE-2019-20006

Published on: 12/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:51 PM UTC

CVE-2019-20006

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

Certain versions of [Ezxml](#) from [Ezxml Project](#) contain the following vulnerability:

An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_char_content puts a pointer to the internal address of a larger block as xml->txt. This is later deallocated (using free), leading to a segmentation fault.

CVE-2019-20006 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
ezXML / Bugs / #15 Using free on not allocated memory block (ezxml_char_content)	Exploit Third Party Advisory sourceforge.net text/html	MISC sourceforge.net/p/ezxml/bugs/15/

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

- [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

[← Previous ID](#)

[Next ID →](#)