

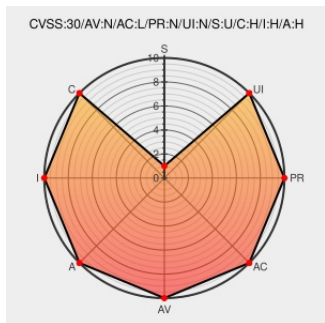


CVE-2018-11210

Published on: 05/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11210

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

Certain versions of [Tinyxml2](#) from [Tinyxml2 Project](#) contain the following vulnerability:

**** DISPUTED **** TinyXML2 6.2.0 has a heap-based buffer over-read in the XMLDocument::Parse function in libtinyxml2.so. NOTE: The tinyxml2 developers have determined that the reported overflow is due to improper use of the library and not a vulnerability in tinyxml2.

CVE-2018-11210 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
heap-buffer-overflow Error In tinyxml2.cpp:2286::strlen() · Issue #675 · leethomason/tinyxml2 · GitHub	github.com text/html	MISC github.com/leethomason/tinyxml2/issues/675#issuecomment-439933437
heap-buffer-overflow Error In	github.com	MISC

tinycl2.cpp:2286::strlen() · Issue #675 · leethomason/tinycl2 · GitHub

text/html

github.com/leethomason/tinycl2/issues/675#issuecomment-462194018

heap-buffer-overflow Error In tinycl2.cpp:2286::strlen() · Issue #675 · leethomason/tinycl2 · GitHub

Third Party Advisorygithub.comtext/html

MISC github.com/leethomason/tinycl2/issues/675

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tinycl2 Project	Tinycl2	6.2.0	All	All	All
Application	Tinycl2 Project	Tinycl2	6.2.0	All	All	All

cpe:2.3:a:tinycl2_project:tinycl2:6.2.0:****:*:*:

cpe:2.3:a:tinycl2_project:tinycl2:6.2.0:****:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→