



CVE-2020-19490

Published on: 07/21/2021 12:00:00 AM UTC

Last Modified on: 07/31/2021 12:27:00 AM UTC

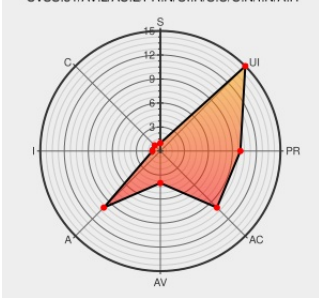
CVE-2020-19490

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H



Certain versions of **Tinyexr** from **Tinyexr Project** contain the following vulnerability:

tinyexr 0.9.5 has a integer overflow over-write in tinyexr::DecodePixelData in tinyexr.h, related to OpenEXR code.

CVE-2020-19490 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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
Make line_no with too large value(2**20) invalid. Fixes #124 · syoyo/tinyexr@a685e33 · GitHub	github.com text/html	MISC github.com/syoyo/tinyexr/commit/a685e332f61cd4e59324bf3f669d36973d64270
Crash on DecodePixelData · Issue #124 ·	github.com	MISC github.com/syoyo/tinyexr/issues/124

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	Tinyexr Project	Tinyexr	0.9.5	All	All	All
<code>cpe:2.3:a:tinyexr_project:tinyexr:0.9.5:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-19490 : tinyexr 0.9.5 has a integer overflow over-write in tinyexr::DecodePixelData in tinyexr.h, related... twitter.com/i/web/status/1...	2021-07-21 18:10:05
 @xanadulinux	CVE-2020-19490 ift.tt/3zjB6jW	2021-07-21 20:52:23
 @Velletron	CVE-2020-19490 ift.tt/3zjB6jW #CVE #Vulnerability	2021-07-21 20:54:15
 @workentin	New vulnerability on the NVD: CVE-2020-19490 ift.tt/3zjB6jW	2021-07-21 21:05:08
 @WesUncensored	New vulnerability on the NVD: CVE-2020-19490 ift.tt/3zjB6jW	2021-07-22 07:33:36
 /r/netcve	CVE-2020-19490	2021-07-21 18:38:27

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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