



CVE-2020-21049

Published on: 09/14/2021 12:00:00 AM UTC

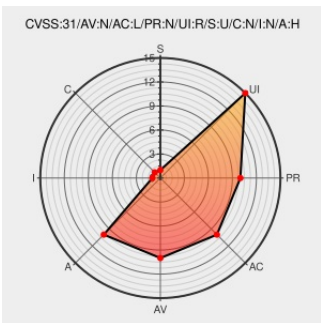
Last Modified on: 09/24/2021 05:08:00 PM UTC

CVE-2020-21049

Source: Mitre

Source: Nist

Print: PDF



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

An invalid read in the `stb_image.h` component of `libsixel` prior to v1.8.5 allows attackers to cause a denial of service (DOS) via a crafted PSD file.

CVE-2020-21049 has been assigned by [M](#) 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
Address Sanitizer: invalid read at <code>stb_image.h:5669</code> · Issue #74 · saitoha/libsixel · GitHub	github.com text/html	MISC github.com/saitoha/libsixel/issues/74
404 — Bitbucket	bitbucket.org	MISC

[text/html](#)bitbucket.org/netbsd/pkgsrc/commits/970a81d31ec7498e04d09b6b7771cef3[Inactive Link](#) [Not Archived](#)Release v1.8.5 security update ·
saitoha/libsixel · GitHub[github.com](#) MISC github.com/saitoha/libsixel/releases/tag/v1.8.5[text/html](#)Introduce
SIXEL_ALLOCATE_BYTES_MAX
macro and limit allocation size
to... · saitoha/libsixel@0b1e0b3 ·
GitHub[github.com](#)

MISC

[text/html](#)github.com/saitoha/libsixel/commit/0b1e0b3f7b44233f84e5c9f512f8c90d6bb1libsixel/ChangeLog at master ·
saitoha/libsixel · GitHub[github.com](#) MISC github.com/saitoha/libsixel/blob/master/ChangeLog[text/html](#)

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	Libsixel Project	Libsixel	All	All	All	All

cpe:2.3:a:libsixel_project:libsixel:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-21049 : An invalid read in the stb_image.h component of libsixel prior to v1.8.5 allows attackers to cause... twitter.com/i/web/status/1...	2021-09-14 16:03:39
@4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2020-21049	2021-09-15 06:55:36

[← Previous ID](#)[Next ID →](#)

© CVE.report 2021 |

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