



CVE-2020-21050

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

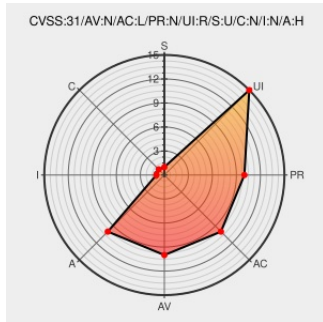
Last Modified on: 09/24/2021 05:17:00 PM UTC

CVE-2020-21050

Source: Mitre

Source: Nist

Print: PDF



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

Libsixel prior to v1.8.3 contains a stack buffer overflow in the function gif_process_raster at fromgif.c.

CVE-2020-21050 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
404 — Bitbucket	bitbucket.org text/html Inactive Link Not Archived	MISC bitbucket.org/netbsd/pkgsrc/commits/a27113e21179cbfbfae0c35f6a9edd6aa498faae
Release v1.8.5 security	github.com	MISC github.com/saitoha/libsixel/releases/tag/v1.8.5

update · saito/ha/libsixel · [text/html](#)
GitHub

AddressSanitizer: stack-
buffer-overflow at
fromgif.c:310 · Issue #75
· saito/ha/libsixel · GitHub

 [MISC github.com/saito/ha/libsixel/issues/75](https://github.com/saito/ha/libsixel/issues/75)

gif loader: check LZW
code size (Issue #75) ·
saito/ha/libsixel@7808a06
· GitHub

 [MISC github.com/saito/ha/libsixel/commit/7808a06b88c11dbc502318cdd51fa374f8cd47ee](https://github.com/saito/ha/libsixel/commit/7808a06b88c11dbc502318cdd51fa374f8cd47ee)

libsixel/ChangeLog at
master · saito/ha/libsixel ·
GitHub

 [MISC github.com/saito/ha/libsixel/blob/master/ChangeLog](https://github.com/saito/ha/libsixel/blob/master/ChangeLog)

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-2020-21050 : Libsixel prior to v1.8.3 contains a stack buffer overflow in the function gif_process_raster at fr... twitter.com/i/web/status/1...	2021-09-14 16:04:06
 @EWS_Bot	Potentially Critical CVE Detected! CVE-2020-21050 Description: CVE-2020-21050 Libsixel prior to v1.8.3 contains a s... twitter.com/i/web/status/1...	2021-09-14 17:00:03
 @4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2020-21050	2021-09-15 06:55:43

[← 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