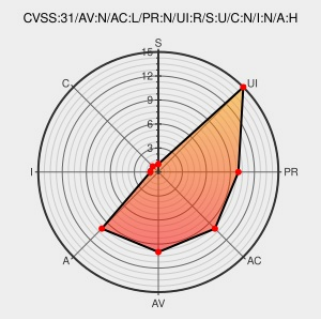
CVE-2020-21050

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 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 · saitoha/libsixel · GitHub	text/html	
AddressSanitizer: stack-buffer-overflow at fromgif.c:310 · Issue #75 · saitoha/libsixel · GitHub	github.com text/html	MISC github.com/saitoha/libsixel/issues/75
gif loader: check LZW code size (Issue #75) · saitoha/libsixel@7808a06 · GitHub	github.com text/html	MISC github.com/saitoha/libsixel/commit/7808a06b88c11dbc502318cdd51fa374f8cd47ee
libsixel/ChangeLog at master · saitoha/libsixel · GitHub	github.com text/html	MISC github.com/saitoha/libsixel/blob/master/ChangeLog

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→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report