



CVE-2019-19777

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-19777
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-13 02:15:00 UTC
Updated	2019-12-18 20:20:00 UTC
Description	stb_image.h (aka the stb image loader) 2.23, as used in libsixel and other products, has a heap-based buffer over-read in s

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libsixel Project	Libsixel	1.8.2	All	All	All
Application	Libsixel Project	Libsixel	1.8.2	All	All	All
Application	Nothings	Stb Image.h	2.23	All	All	All
Application	Nothings	Stb Image.h	2.23	All	All	All

References

Reference	Source	Link	Tags
heap-buffer-overflow in stbi__load_main at stb_image.h:5580 · Issue #109 · saitoha/libsixel · GitHub	MISC	github.com	Exploit, Th
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)