VDB-354253 · CVE-2026-5185 · GCVE-100-354253

NOTHINGS STB_IMAGE UP TO 2.30 MULTI-FRAME GIF FILE STB_IMAGE.H STBI__GIF_LOAD_NEXT HEAP-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	3.66-

Summary

A vulnerability marked as critical has been reported in Nothings stb_image up to 2.30. This impacts the function `stbi__gif_load_next` of the file *stb_image.h* of the component *Multi-frame GIF File Handler*. This manipulation causes heap-based overflow. This vulnerability appears as CVE-2026-5185. The attack requires local access. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability has been found in Nothings stb_image up to 2.30 and classified as critical. Affected by this vulnerability is the function `stbi__gif_load_next` of the file *stb_image.h* of the component *Multi-frame GIF File Handler*. The manipulation with an unknown input leads to a heap-based overflow vulnerability. The CWE definition for the vulnerability is CWE-122. A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). As an impact it is known to affect confidentiality, integrity, and availability.

This vulnerability is known as CVE-2026-5185. The exploitation appears to be easy. An attack has to be approached locally. Technical details and also a public exploit are known.

It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

See VDB-185212, VDB-185214, VDB-191572 and VDB-195852 for similar entries.

Product

Vendor

- Nothings

Name

- stb_image

Version

- 2.0
- 2.1
- 2.2
- 2.3
- 2.4
- 2.5
- 2.6
- 2.7
- 2.8
- 2.9
- 2.10
- 2.11
- 2.12
- 2.13

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Heap-based overflow
CWE: CWE-122 / CWE-119
CAPEC: 🔒
ATT&CK: 🔒

Physical: Partially
Local: Yes
Remote: No

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

03/30/2026		Advisory disclosed
03/30/2026	+0 days	VulDB entry created
03/30/2026	+0 days	VulDB entry last update

Sources

Status: Not defined

CVE: CVE-2026-5185 (🔒)
GCVE (CVE): GCVE-0-2026-5185
GCVE (VulDB): GCVE-100-354253
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/30/2026 09:23 PM
Changes: 03/30/2026 09:23 PM (55)
Complete: 🔍
Submitter: d0razi
Cache ID: 52:FE5:179

Submit

Accepted

- Submit #780390: nothings stb stb_image.h <= 2.30 Heap-based Buffer Overflow (by d0razi)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa