



VDB-354254 · CVE-2026-5186 · GCVE-100-354254

# NOTHINGS STB UP TO 2.30 MULTI-FRAME GIF FILE STB\_IMAGE.H STBI\_LOAD\_GIF\_MAIN DOUBLE FREE

CVSS Meta Temp Score ⓘ

4.8

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.29-

## Summary

A vulnerability described as [critical](#) has been identified in [Nothings stb up to 2.30](#). Affected is the function `stbi_load_gif_main` of the file `stb_image.h` of the component *Multi-frame GIF File Handler*. Such manipulation leads to double free. This vulnerability is traded as [CVE-2026-5186](#). An attack has to be approached locally. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability was found in [Nothings stb up to 2.30](#) and classified as [critical](#). Affected by this issue is the function `stbi_load_gif_main` of the file `stb_image.h` of the component *Multi-frame GIF File Handler*. The manipulation with an unknown input leads to a double free vulnerability. Using CWE to declare the problem leads to [CWE-415](#). The product calls `free()` twice on the same memory address, potentially leading to modification of unexpected memory locations. Impacted is confidentiality, integrity, and availability.

This vulnerability is handled as [CVE-2026-5186](#). The exploitation is known to be easy. Local access is required to approach this attack. Technical details as well as 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.

The entries [VDB-185214](#), [VDB-191572](#), [VDB-195852](#) and [VDB-197475](#) are related to this item.

## Product

### Vendor

- [Nothings](#)

### Name

- [stb](#)

### 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](#)
- [2.14](#)

### 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:** Double free

**CWE:** [CWE-415](#) / [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-2026-5186](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5186](#)

GCVE (VulDB): [GCVE-100-354254](#)

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: 20:A1E:179

## Submit

Accepted

- [Submit #780395](#): nothings stb stb\_image.h <= 2.30 Double Free (by d0razi)

## Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)