



# CVE-2021-26826

Published on: 02/08/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:29:03 PM UTC

## CVE-2021-26826

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Godot Engine](#) from [Godotengine](#) contain the following vulnerability:

A stack overflow issue exists in Godot Engine up to v3.2 and is caused by improper boundary checks when loading .TGA image files. Depending on the context of the application, attack vector can be local or remote, and can lead to code execution and/or system crash.

CVE-2021-26826 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                        | Tags                                                                                                                     | Link                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fix a crash in the TGA loader with malformed input by hpvb · Pull Request #45701 · | <a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="https://github.com/godotengine/godot/pull/45701/commits/403e4fd08b0b212e96f53d926e6273e0745eaa5">github.com/godotengine/godot/pull/45701/commits/403e4fd08b0b212e96f53d926e6273e0745eaa5</a> |

godotengine/godot  
· GitHub

Fix a crash in the TGA loader with malformed input by hpvb · Pull Request #45701 · godotengine/godot · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC [github.com/godotengine/godot/pull/45701](https://github.com/godotengine/godot/pull/45701)

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](mailto: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                                | <a href="#">Godotengine</a> | <a href="#">Godot Engine</a> | All     | All    | All     | All      |
| cpe:2.3:a:godotengine:godot_engine:*****:: |                             |                              |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→