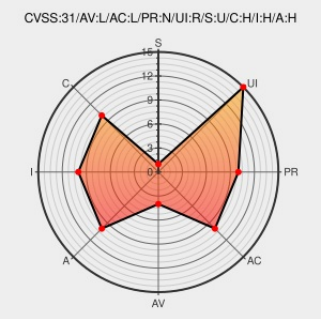
CVE-2021-26825

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

Last Modified on: 03/23/2021 11:29:01 PM UTC

CVE-2021-26825

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Godot Engine from Godotengine contain the following vulnerability:

An integer overflow issue exists in Godot Engine up to v3.2 that can be triggered when loading specially crafted.TGA image files. The vulnerability exists in ImageLoaderTGA::load_image() function at line: const size_t buffer_size = (tga_header.image_width * tga_header.image_height) * pixel_size; The bug leads to Dynamic stack buffer overflow. 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-2021-26825 has been assigned by 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
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[3.2] Fix a crash in the TGA loader with malformed input by bruvb	Patch	MISC

[3.2] Fix a crash in the TGA loader with malformed input by hpvb · Pull Request #45702 · godotengine/godot · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/godotengine/godot/pull/45702/files
[3.2] Fix a crash in the TGA loader with malformed input by hpvb · Pull Request #45702 · godotengine/godot · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/godotengine/godot/pull/45702

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Godotengine	Godot Engine	All	All	All	All

cpe:2.3:a:godotengine:godot_engine:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→