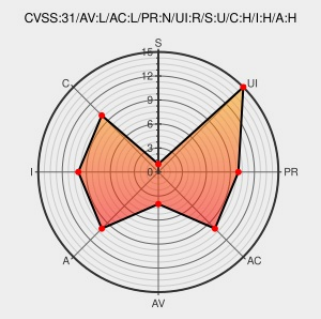
CVE-2021-26826

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 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
Fix a crash in the TGA loader with malformed input by hpvb · Pull Request #45701 ·	Patch Third Party Advisory github.com text/html	MISC github.com/godotengine/godot/pull/45701/commits/403e4fd08b0b212e96f53d926e6273e0745eaa5

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

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→