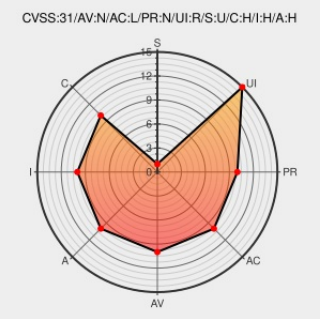
CVE-2020-28248

Published on: 02/19/2021 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-28248

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



Certain versions of Png-img from Png-img Project contain the following vulnerability:

An integer overflow in the PngImg::InitStorage_() function of png-img before 3.1.0 leads to an under-allocation of heap memory and subsequently an exploitable heap-based buffer overflow when loading a crafted PNG file.

CVE-2020-28248 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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
Handle image size overflow · gemini-testing/png-img@14ac462 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/gemini-testing/png-img/commit/14ac462a32ca4b3b78f56502ac976d5b0222ce3d

GHSL-2020-142: Heap memory corruption in png-img - CVE-2020-28248 - GitHub Security Lab	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC securitylab.github.com/advisories/GHSL-2020-142-gemini-png-img
GitHub - gemini-testing/png-img: Lite libpng wrapper for node.js	Product github.com text/html	MISC github.com/gemini-testing/png-img
Comparing v3.0.0...v3.1.0 · gemini-testing/png-img · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/gemini-testing/png-img/compare/v3.0.0...v3.1.0

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Png-img Project	Png-img	All	All	All	All
Application	Png-img Project	Png-img	All	All	All	All

cpe:2.3:a:png-img_project:png-img:*:*:*:*:*:*:*:*:

cpe:2.3:a:png-img_project:png-img:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→