



CVE-2021-39178

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-39178
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-31 00:15:00 UTC
Updated	2021-09-08 13:26:00 UTC
Description	Next.js is a React framework. Versions of Next.js between 10.0.0 and 11.0.0 contain a cross-site scripting vulnerability. In o

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vercel	Next.js	All	All	All	All

References

Reference	Source	Link
XSS in Image Optimization API for Next.js versions between 10.0.0 and 11.1.0 · Advisory · vercel/next.js · GitHub	CONFIRM	github.com
Release v11.1.1 · vercel/next.js · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981298](#) Nodejs (npm) Security Update for next (GHSA-9gr3-7897-pp7m)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)