



CVE-2020-5284

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

Summary

CVE	CVE-2020-5284
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-30 22:15:00 UTC
Updated	2020-04-01 20:08:00 UTC
Description	Next.js versions before 9.3.2 have a directory traversal vulnerability. Attackers could craft special requests to access files in

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Directory Traversal in Next.js versions below 9.3.2 · Advisory · vercel/next.js · GitHub	CONFIRM	github.com	Third Party Advisory
Release v9.3.2 · zeit/next.js · GitHub	MISC	github.com	Release Notes
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983124](#) Nodejs (npm) Security Update for next (GHSA-fq77-7p7r-83rj)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report