



CVE-2023-46298

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

Summary

CVE	CVE-2023-46298
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-22 03:15:00 UTC
Updated	2023-10-28 03:30:00 UTC
Description	Next.js before 13.4.20-canary.13 lacks a cache-control header and thus empty prefetch responses may sometimes be cach

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vercel	Next.js	All	All	All	All
Application	Vercel	Next.js	13.4.20	canary0	All	All
Application	Vercel	Next.js	13.4.20	canary1	All	All
Application	Vercel	Next.js	13.4.20	canary10	All	All
Application	Vercel	Next.js	13.4.20	canary11	All	All
Application	Vercel	Next.js	13.4.20	canary12	All	All
Application	Vercel	Next.js	13.4.20	canary2	All	All
Application	Vercel	Next.js	13.4.20	canary3	All	All
Application	Vercel	Next.js	13.4.20	canary4	All	All
Application	Vercel	Next.js	13.4.20	canary5	All	All
Application	Vercel	Next.js	13.4.20	canary6	All	All
Application	Vercel	Next.js	13.4.20	canary7	All	All
Application	Vercel	Next.js	13.4.20	canary8	All	All
Application	Vercel	Next.js	13.4.20	canary9	All	All

References

Reference

Missing cache control directive for server side props response when using middleware and prefetch · Issue #45301 · vercel/next.js · GitHub

Comparing v13.4.20-canary.12...v13.4.20-canary.13 · vercel/next.js · GitHub

Add cache control header for prefetch empty responses by remorses · Pull Request #54732 · vercel/next.js · GitHub

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995699](#) NodeJs (Npm) Security Update for next (GHSA-c59h-r6p8-q9wc)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)