



CVE-2021-23518

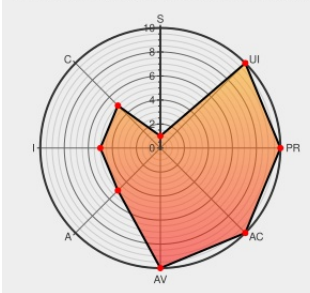
Published on: 01/21/2022 12:00:00 AM UTC

Last Modified on: 02/03/2023 07:16:00 PM UTC

CVE-2021-23518

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P



Certain versions of [Cached-path-relative](#) from [Cached-path-relative Project](#) contain the following vulnerability:

The package `cached-path-relative` before 1.1.0 are vulnerable to Prototype Pollution via the cache variable that is set as `{}` instead of `Object.create(null)` in the `cachedPathRelative` function, which allows access to the parent prototype properties when the object is used to create the cached relative path. When using the origin path as

`__proto__`, the attribute of the object is accessed instead of a path. **Note:** This vulnerability derives from an incomplete fix in <https://security.snyk.io/vuln/SNYK-JS-CACHEDPATHRELATIVE-72573>

CVE-2021-23518 has been assigned by report@snyk.io to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Prototype Pollution in cached-path-relative CVE-2021-23518 Snyk	snyk.io text/html	 MISC snyk.io/vuln/SNYK-JS-CACHEDPATHRELATIVE-2342653
Prototype Pollution in org.webjars.npm:cached-path-relative CVE-2021-23518 Snyk	snyk.io text/html	 MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2348246
Fix other instances of prototype pollution vulnerability · ashaffer/cached-path-relative@40c73bf · GitHub	github.com text/html	 MISC github.com/ashaffer/cached-path-relative/commit/40c73bf70c58add5aec7d11e4f36b93d144bb760
[SECURITY] [DLA 3221-1] node-cached-path-relative security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20221204 [SECURITY] [DLA 3221-1] node-cached-path-relative security update

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[179425](#) Debian Security Update for node-cached-path-relative (CVE-2021-23518)

[181288](#) Debian Security Update for node-cached-path-relative (DLA 3221-1)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cached-path-relative Project	Cached-path-relative	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
cpe:2.3:a:cached-path-relative_project:cached-path-relative:*:*:*:*:node.js:*:*:						
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						

Discovery Credit

P.Adithya Srinivas

Masudul Hasan Masud Bhuiyan

Cristian-Alexandru Staicu

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23518 : The package cached-path-relative before 1.1.0 are vulnerable to Prototype Pollution via the cache... twitter.com/i/web/status/1...	2022-01-21 20:12:59

 @xanadulinux	CVE-2021-23518 ift.tt/3FK8Eux	2022-01-21 22:06:05
 /r/netcve	CVE-2021-23518	2022-01-21 21:54:38

[< Previous ID](#)
[Next ID >](#)

© [CVE.report](#) 2023   |

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](#).

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