



CVE-2021-23507

Published on: 02/04/2022 12:00:00 AM UTC

Last Modified on: 02/09/2022 05:39:00 PM UTC

CVE-2021-23507

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

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



Certain versions of [Object-path-set](#) from [Skratchdot](#) contain the following vulnerability:

The package object-path-set before 1.0.2 are vulnerable to Prototype Pollution via the setPath method, as it allows an attacker to merge object prototypes into it. *Note:* This vulnerability derives from an incomplete fix in <https://security.snyk.io/vuln/SNYK-JS-OBJECTPATHSET-607908>

CVE-2021-23507 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
fix new prototype pollution vulnerability - skratshdot/object-path-set@2d67a71 · GitHub	github.com text/html	MISC github.com/skratchdot/object-path-set/commit/2d67a714159c4099589b6661fa84e6d2adc31761
JavaScript type confusion: Bypassed input validation	snyk.io	MISC: snyk.io/blog/remediate-javascript-type-confusion-bypassed-

javascript type confusion. Bypassed input validation (and how to remediate) | Snyk

snyk.io

text/html

MISC snyk.io/blog/remediate-javascript-type-confusion-bypassed-input-validation/

Prototype Pollution in object-path-set | CVE-2021-23507 | Snyk

snyk.io

text/html

MISC snyk.io/vuln/SNYK-JS-OBJECTPATHSET-2388576

object-path-set/index.js at 577f5299fed15bb9edd11c940ff3cf0b9f4748d5 · skratchdot/object-path-set · GitHub

github.com

text/html

MISC github.com/skratchdot/object-path-set/blob/577f5299fed15bb9edd11c940ff3cf0b9f4748d5/index.js%23L8

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Skratchdot	Object-path-set	All	All	All	All
cpe:2.3:a:skratchdot:object-path-set:****:****:*						

Discovery Credit

P.Adithya Srinivas

Masudul Hasan Masud Bhuiyan

Cristian-Alexandru Staicu

Alessio Della Libera

Social Mentions		
Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23507 : The package object-path-set before 1.0.2 are vulnerable to Prototype Pollution via the setPath met... twitter.com/i/web/status/1...	2022-02-04 20:14:33
/r/netcve	CVE-2021-23507	2022-02-04 21:38:41

← Previous ID

Next ID →

