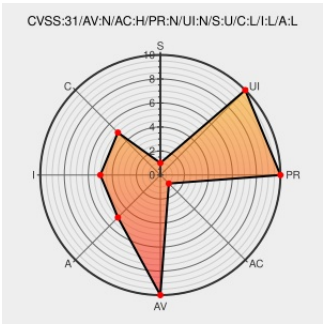
CVE-2021-23434

Published on: 08/27/2021 12:00:00 AM UTC

Last Modified on: 01/30/2023 06:24:00 PM UTC

CVE-2021-23434

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

This affects the package object-path before 0.11.6. A type confusion vulnerability can lead to a bypass of CVE-2020-15256 when the path components used in the path parameter are arrays. In particular, the condition currentPath === '__proto__' returns false if currentPath is ['__proto__']. This is because the === operator returns always false when the type of the operands is different.

CVE-2021-23434 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	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
GitHub - mariocasciaro/object-path: A tiny JavaScript utility to access deep properties using a path (for Node and the	github.com text/html	MISC github.com/mariocasciaro/object-path%230116

Browser)		
Fix prototype pollution when path components are not strings · mariocasciaro/object-path@7bdf4ab · GitHub	github.com text/html	MISC github.com/mariocasciaro/object-path/commit/7bdf4abefd102d16c163d633e8994ef154cab9eb
Prototype Pollution in object-path | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-OBJECTPATH-1569453
[SECURITY] [DLA 3291-1] node-object-path security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230129 [SECURITY] [DLA 3291-1] node-object-path security update
Prototype Pollution in org.webjars.npm:object-path | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1570423

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

179904 Debian Security Update for node-object-path (CVE-2021-23434)

181517 Debian Security Update for node-object-path (DLA 3291-1)

199249 Ubuntu Security Notification for object-path Vulnerabilities (USN-5967-1)

980535 Nodejs (npm) Security Update for object-path (GHSA-v39p-96qg-c8rf)

Exploit/POC from Github

PoC for exploiting CVE-2021-23434 : This affects the package object-path before 0.11.6. A type confusion vulnerabilit…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Object-path Project	Object-path	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:a:object-path_project:object-path:*:*:*:*:*:node.js:*:*:

Discovery Credit

Alessio Della Libera of Snyk Research Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23434 : This affects the package object-path before 0.11.6. A type confusion vulnerability can lead to a… twitter.com/i/web/status/1…	2021-08-27 16:56:52

@threatmeter	CVE-2021-23434 This affects the package object-path before 0.11.6. A type confusion vulnerability can lead to a byp… twitter.com/i/web/status/1…	2021-08-28 09:09:32

← 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 registred 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