



CVE-2020-15256

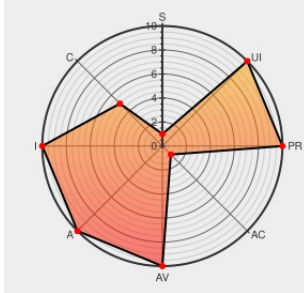
Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:20:00 PM UTC

CVE-2020-15256 - advisory for GHSA-cwx2-736x-mf6w

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

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



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

A prototype pollution vulnerability has been found in ``object-path`` $\leq 0.11.4$ affecting the ``set()`` method. The vulnerability is limited to the ``includeInheritedProps`` mode (if version $\geq 0.11.0$ is used), which has to be explicitly enabled by creating a new instance of ``object-path`` and setting the option ``includeInheritedProps: true``, or by using the default

``withInheritedProps`` instance. The default operating mode is not affected by the vulnerability if version $\geq 0.11.0$ is used. Any usage of ``set()`` in versions $< 0.11.0$ is vulnerable. The issue is fixed in `object-path` version 0.11.5 As a workaround, don't use the ``includeInheritedProps: true`` options or the ``withInheritedProps`` instance if using a version $\geq 0.11.0$.

CVE-2020-15256 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [mariocasciaro](#) - `object-path` version $< 0.11.5$

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: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Fix prototype pollution in set() · mariocasciaro/object-path@2be3354 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/mariocasciaro/object-path/commit/2be3354c6c46215c7635eb1b76d80f1319403c68
Prototype pollution affecting the set() method using the includeInheritedProps mode · Advisory · mariocasciaro/object-path · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/mariocasciaro/object-path/security/advisories/GHSA-cwx2-736x-mf6w

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

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

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

980065 Nodejs (npm) Security Update for object-path (GHSA-cwx2-736x-mf6w)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Object-path Project	Object-path	All	All	All	All
Application	Object-path Project	Object-path	All	All	All	All
cpe:2.3:a:object-path_project:object-path:*.*.*.*:node.js:*.*:						
cpe:2.3:a:object-path_project:object-path:*.*.*.*:node.js:*.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID→		

