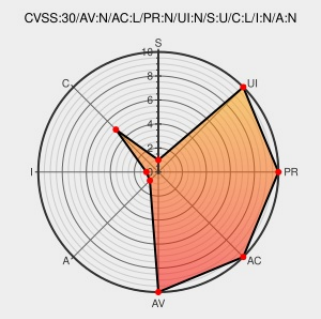
CVE-2018-17175

Published on: 09/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:19 PM UTC

CVE-2018-17175

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



Certain versions of Marshmallow from Marshmallow Project contain the following vulnerability:

In the marshmallow library before 2.15.1 and 3.x before 3.0.0b9 for Python, the schema "only" option treats an empty list as implying no "only" option, which allows a request that was intended to expose no fields to instead expose all fields (if the schema is being filtered dynamically using the "only" option, and there is a user role that produces an empty value for "only").

CVE-2018-17175 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Empty Only Treated as None · Issue #772 · marshmallow-code/marshmallow · GitHub	Issue Tracking, Third Party Advisory	MISC github.com/marshmallow-code/marshmallow/issues/772

	github.com text/html	
Fix #772 Empty Only Treated as None / 2.x-line by lafrech · Pull Request #782 · marshmallow-code/marshmallow · GitHub	Third Party Advisory github.com text/html	MISC github.com/marshmallow-code/marshmallow/pull/782
Fix #772 Empty Only Treated as None by lafrech · Pull Request #777 · marshmallow-code/marshmallow · GitHub	Third Party Advisory github.com text/html	MISC github.com/marshmallow-code/marshmallow/pull/777

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

981148 Python (pip) Security Update for marshmallow (GHSA-9q2p-fj49-vpxj)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Marshmallow Project	Marshmallow	All	All	All	All
Application	Marshmallow Project	Marshmallow	All	All	All	All
Application	Marshmallow Project	Marshmallow	All	All	All	All
Application	Marshmallow Project	Marshmallow	All	All	All	All

cpe:2.3:a:marshmallow_project:marshmallow:*:*:*:*:*:*:*:*:

cpe:2.3:a:marshmallow_project:marshmallow:*:*:*:*:*:python:*:*:

cpe:2.3:a:marshmallow_project:marshmallow:*:*:*:*:*:*:*:*:

cpe:2.3:a:marshmallow_project:marshmallow:*:*:*:*:*:python:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→