

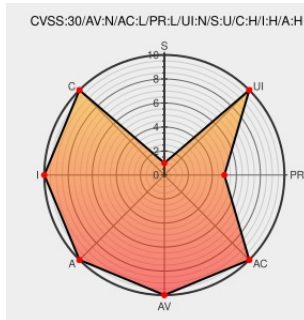


CVE-2016-10533

Published on: 05/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:00 PM UTC

CVE-2016-10533

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

Certain versions of [Express-restify-mongoose](#) from [Express-restify-mongoose Project](#) contain the following vulnerability:

express-restify-mongoose is a module to easily create a flexible REST interface for mongoose models. express-restify-mongoose 2.4.2 and earlier and 3.0.X through 3.0.1 allows a malicious user to send a request for `GET /User?distinct=password` and get all the passwords for all the users in the database, despite the field being set to private.

This can be used for other private data if the malicious user knew what was set as private for specific routes.

CVE-2016-10533 has been assigned by support@hackerone.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **HackerOne** - **express-restify-mongoose node module** version `<= 2.4.2 || >= 3.0.0 <=3.0.1`

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description

Leaking private/protected data · Issue #252 · florianholzapfel/express-registry-mongoose · GitHub

Tags

Issue Tracking

Third Party Advisory

github.com

text/html

Link

MISC

github.com/florianholzapfel/express-registry-mongoose/issues/252

Overview

Exploit

Third Party Advisory

nodesecurity.io

text/html

S

MISC

nodesecurity.io/advisories/92

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

983935 Nodejs (npm) Security Update for express-registry-mongoose (GHSA-cgix-mwpx-47jv)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Express-registry-mongoose Project	Express-registry-mongoose	All	All	All	All
Application	Express-registry-mongoose Project	Express-registry-mongoose	All	All	All	All

cpe:2.3:a:express-registry-mongoose_project:express-registry-mongoose:*.***.***:node.js:***:

cpe:2.3:a:express-registry-mongoose_project:express-registry-mongoose:*.***.***:node.js:***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →