

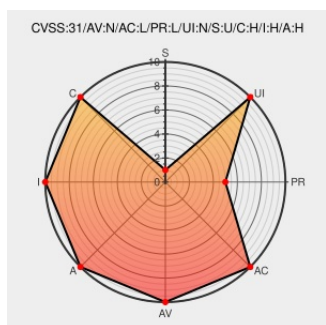


CVE-2020-35666

Published on: 12/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:47 PM UTC

CVE-2020-35666

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

Certain versions of [Steedos](#) from [Steedos](#) contain the following vulnerability:

Steedos Platform through 1.21.24 allows NoSQL injection because the `/api/collection/findone` implementation in `server/packages/steedos_base.js` mishandles `req.body` validation, as demonstrated by MongoDB operator attacks such as an `X-User-Id[$ne]=1` value.

CVE-2020-35666 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

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: **6.5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Mongodb NoSQL 注入问题 · Issue #1245 · steedos/steedos-platform · GitHub

[Exploit](#)

[Vendor Advisory](#)

[github.com](#)

[MISC github.com/steedos/steedos-platform/issues/1245](#)

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	Steedos	Steedos	All	All	All	All
cpe:2.3:a:steedos:steedos:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← 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 registered 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