



CVE-2022-35956

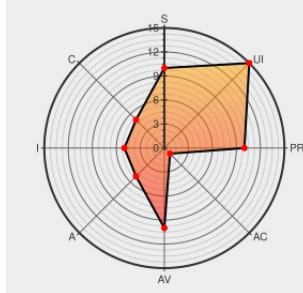
Published on: Not Yet Published

Last Modified on: 08/16/2022 04:09:00 PM UTC

CVE-2022-35956 - advisory for GHSA-33wh-w4m7-c6r8

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

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



Certain versions of [Update By Case](#) from [Update By Case Project](#) contain the following vulnerability:

This Rails gem adds two methods to the ActiveRecord::Base class that allow you to update many records on a single database hit, using a case sql statement for it. Before version 0.1.3 `update\_by\_case` gem used custom sql strings, and it was not sanitized, making it vulnerable to sql injection. Upgrade to version $\geq 0.1.3$ that uses `Arel` instead to construct the resulting sql statement, with sanitized sql.

CVE-2022-35956 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **camilova** - **activerecord-update-by-case** version $< 0.1.3$

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

CVE References

Description	Tags	Link
Release v0.1.3-stable · camilova/activerecord-update-by-case · GitHub	github.com text/html	MISC github.com/camilova/activerecord-update-by-case/releases/tag/v0.1.3-stable
update_by_case before 0.1.3 can be vulnerable to sql injection · Advisory · camilova/activerecord-update-by-case · GitHub	github.com text/html	CONFIRM github.com/camilova/activerecord-update-by-case/security/advisories/GHSA-33wh-w4m7-c6r8

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	Update By Case Project	Update By Case	All	All	All	All
cpe:2.3:a:update_by_case_project:update_by_case:*:*:*:*:ruby:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-35956 : This Rails gem adds two methods to the ActiveRecord::Base class that allow you to update many reco... twitter.com/i/web/status/1...	2022-08-12 20:54:54
 /r/netcve	CVE-2022-35956	2022-08-12 21:38:29

[← 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](#)