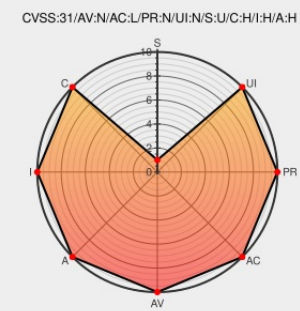
CVE-2017-20166

Published on: Not Yet Published

Last Modified on: 11/07/2023 02:43:00 AM UTC

CVE-2017-20166

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



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

Ecto 2.2.0 lacks a certain protection mechanism associated with the interaction between is_nil and raise.

CVE-2017-20166 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
Add support for clauses with nil values in `Repo.get_by(!)/2` by tlux · Pull Request #2125 · elixir-ecto/ecto · GitHub	github.com text/html	MISC github.com/elixir-ecto/ecto/pull/2125
Google Groups	groups.google.com text/html	MISC groups.google.com/forum/#!topic/elixir-ecto/0m4NPfg_MMU
Revert "Add support for clauses with nil values in `Repo.get_by(!)/2`… · elixir-ecto/ecto@db55b0c · GitHub	github.com text/html	MISC github.com/elixir-ecto/ecto/commit/db55b0cba6525c24ebddc88ef9ae0c1c00620250
Missing `is_nil` requirement · GHSA-2xxx-fhc8-9qvq · GitHub Advisory Database · GitHub	github.com text/html	MISC github.com/advisories/GHSA-2xxx-fhc8-9qvq

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	Ecto Project	Ecto	2.2.0	All	All	All

cpe:2.3:a:ecto_project:ecto:2.2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report