



CVE-2021-43850

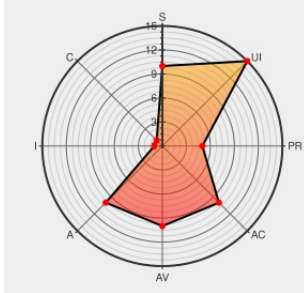
Published on: Not Yet Published

Last Modified on: 01/14/2022 02:50:00 AM UTC

CVE-2021-43850 - advisory for GHSA-59jr-pj65-qmvr

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

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



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

Discourse is an open source platform for community discussion. In affected versions admins users can trigger a Denial of Service attack via the `/message-bus/\_diagnostics` path. The impact of this vulnerability is greater on multisite Discourse instances (where multiple forums are served from a single application server) where any admin user on any of the forums are able to visit the `/message-bus/\_diagnostics` path. The problem has been patched. Please upgrade to 2.8.0.beta10 or 2.7.12. No workarounds for this issue exist.

CVE-2021-43850 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [discourse](#) - **discourse** version < 2.7.12

Affected Vendor/Software: [discourse](#) - **discourse** version >= 2.8.0.beta, < 2.8.0.beta10

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

CVE References

Description	Tags	Link
SECURITY: Disable MessageBus::Diagnostics. · discourse/discourse@7a8ec12 · GitHub	github.com text/html	 MISC github.com/discourse/discourse/commit/7a8ec129fb54f188b2da6588c9d24d3a36eb0d39
MessageBus::Diagnostics route susceptible to DoS · Advisory · discourse/discourse · GitHub	github.com text/html	 CONFIRM github.com/discourse/discourse/security/advisories/GHSA-59jr-pj65-qmvr

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	Discourse	Discourse	All	All	All	All
Application	Discourse	Discourse	2.8.0	beta1	All	All
Application	Discourse	Discourse	2.8.0	beta2	All	All
Application	Discourse	Discourse	2.8.0	beta3	All	All
Application	Discourse	Discourse	2.8.0	beta4	All	All
Application	Discourse	Discourse	2.8.0	beta5	All	All
Application	Discourse	Discourse	2.8.0	beta6	All	All
Application	Discourse	Discourse	2.8.0	beta7	All	All
Application	Discourse	Discourse	2.8.0	beta8	All	All
Application	Discourse	Discourse	2.8.0	beta9	All	All

```
cpe:2.3:a:discourse:discourse:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:discourse:discourse:2.8.0:beta1:*:*:*:*:*:
```

```
cpe:2.3:a:discourse:discourse:2.8.0:beta2:*:*:*:*:*:
```

cpe:2.3:a:discourse:discourse:2.8.0:beta3:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.8.0:beta4:****.*.*.*:

```
cpe:2.3:a:discourse:discourse:2.8.0:beta5::*:.*
```

```
ope-2.0-a-discourse/discourse-2.0.0-beta6: . . . . .
```

```
ope-2.0-a-discourse/discourse-2.0.0-beta6: ****
```

cpe:2.3:a:discourse:discourse:2.8.0:betab:.....

cpe:2.3:a:discourse:discourse:2.8.0:beta8:*****:

cpe:2.3:a:discourse:discourse:2.8.0:beta9:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-43850 : Discourse is an open source platform for community discussion. In affected versions admins users c... twitter.com/i/web/status/1...	2022-01-04 19:42:09

← Previous ID

Next ID→