

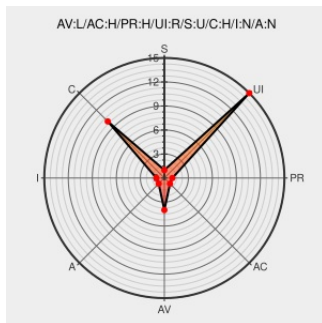


CVE-2020-26416

Published on: 12/10/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-26416

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

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

Information disclosure in Advanced Search component of GitLab EE starting from 8.4 results in exposure of search terms via Rails logs. This affects versions ≥ 8.4 to $< 13.4.7$, ≥ 13.5 to $< 13.5.5$, and ≥ 13.6 to $< 13.6.2$.

CVE-2020-26416 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab EE** version ≥ 8.4 to $< 13.4.7$

Affected Vendor/Software: **GitLab** - **GitLab EE** version ≥ 13.5 to $< 13.5.5$

Affected Vendor/Software: **GitLab** - **GitLab EE** version ≥ 13.6 to $< 13.6.2$

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link				
Not Found	Broken Link gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/244495				
2020/CVE-2020-26416.json · master · GitLab.org / cves · GitLab	Third Party Advisory gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26416.json				
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	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	All	All	All	All
cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						
Discovery Credit						
This vulnerability has been discovered internally by the GitLab team						
← Previous ID			Next ID →			