



CVE-2018-16049

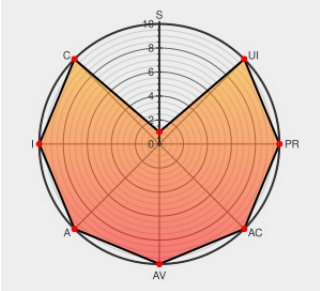
Published on: 10/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16049

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

An issue was discovered in GitLab Community and Enterprise Edition before 11.0.6, 11.1.x before 11.1.5, and 11.2.x before 11.2.2. There is Sensitive Data Disclosure in Sidekiq Logs through an Error Message.

CVE-2018-16049 has been assigned by [M](#) 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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Credentials used for repository import are visible inside the Sidekiq logs (Background Jobs) (#49272) · Issues · GitLab.org / GitLab FOSS · GitLab	Exploit Vendor Advisory gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/gitlab-ce/issues/49272

Credentials outputted as plain text in the sidekiq log file. (#46967) · Issues · GitLab.org / GitLab FOSS · GitLab

Exploit
Vendor Advisory
gitlab.com
text/html

CONFIRM gitlab.com/gitlab-org/gitlab-ce/issues/46967

404 | GitLab

Vendor Advisory
about.gitlab.com
text/html
Inactive Link Not Archived

CONFIRM
about.gitlab.com/2018/08/28/security-release-gitlab-11-dot-2-dot-2-released/

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:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →