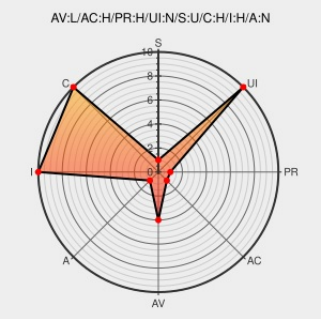
CVE-2021-22194

Published on: 03/26/2021 12:00:00 AM UTC

Last Modified on: 09/14/2021 04:51:00 PM UTC

CVE-2021-22194

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

In all versions of GitLab, marshalled session keys were being stored in Redis.

CVE-2021-22194 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **<13.7.8**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.8, <13.8.5**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.9, <13.9.2**

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	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/262107
2021/CVE-2021-22194.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22194.json

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

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→