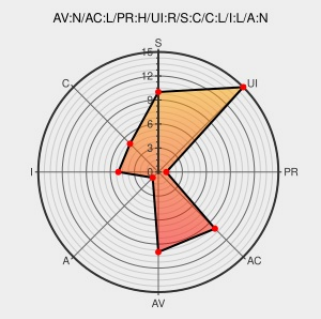
CVE-2020-13328

Published on: 09/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:43 PM UTC

CVE-2020-13328

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

An issue has been discovered in GitLab affecting versions prior to 13.1.2, 13.0.8 and 12.10.13. GitLab was vulnerable to a stored XSS by using the PyPi files API.

CVE-2020-13328 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=12.0, <12.10.13**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.0, <13.0.8**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.1, <13.1.2**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
2020/CVE-2020-13328.json · master · GitLab.org / cves · GitLab	Vendor Advisory gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13328.json
Stored XSS on PyPi simple API endpoint (#215640) · Issues · GitLab.org / GitLab · GitLab	Exploit Vendor Advisory gitlab.com text/html	MISC gitlab.com/gitlab-org/gitlab/-/issues/215640

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:*:*:*:*:*:*:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:*:

Discovery Credit

Thanks [@vakzz](https://hackerone.com/vakzz) for responsibly reporting this vulnerability to us.

← Previous ID

Next ID→