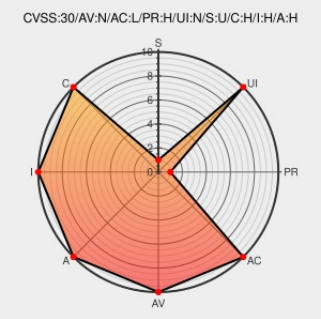
CVE-2017-0925

Published on: 03/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-0925

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Gitlab Enterprise Edition version 10.1.0 is vulnerable to an insufficiently protected credential issue in the project service integration API endpoint resulting in an information disclosure of plaintext password.

CVE-2017-0925 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **GitLab** - **GitLab Community and Enterprise Editions** version **8.10.6 - 10.1.5 Fixed in 10.1.6**

Affected Vendor/Software: **GitLab** - **GitLab Community and Enterprise Editions** version **10.2.0 - 10.2.5 Fixed in 10.2.6**

Affected Vendor/Software: **GitLab** - **GitLab Community and Enterprise Editions** version **10.3.0 - 10.3.3 Fixed in 10.3.4**

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4145-1 gitlab	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4145
GitLab Security Release: 10.3.4, 10.2.6, and 10.1.6 | GitLab	Release Notes Vendor Advisory about.gitlab.com text/html	CONFIRM about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/
API exposes plain text password for service integrations (#3847) · Issues · GitLab.org / GitLab · GitLab	Issue Tracking gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/gitlab-ee/issues/3847

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
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
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:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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:*:*:*:

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→