



CVE-2019-5464

Published on: 01/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:00 PM UTC

CVE-2019-5464

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

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

A flawed DNS rebinding protection issue was discovered in GitLab CE/EE 10.2 and later in the `url\_blocker.rb` which could result in SSRF where the library is utilized.

CVE-2019-5464 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [h1](#) **GitLab - GitLab CE/EE version Affects GitLab CE/EE 10.2 and later**

Affected Vendor/Software: [h1](#) **GitLab - GitLab CE/EE version Fixed in 12.1.2 in 12.0.4 and in 11.11.6**

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: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
-------------	------	------

Server Side Request Forgery mitigation bypass (#63959) · Issues · GitLab.org / GitLab FOSS · GitLab	Exploit Vendor Advisory gitlab.com text/html	 MISC gitlab.com/gitlab-org/gitlab-ce/issues/63959
HackerOne	Permissions Required hackerone.com text/html	 MISC hackerone.com/reports/632101
GitLab Security Release: 12.1.2, 12.0.4, and 11.11.7 GitLab	Patch Release Notes Vendor Advisory about.gitlab.com text/html	 MISC about.gitlab.com/releases/2019/07/29/security-release-gitlab-12-dot-1-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

Social Mentions

Source	Title	Posted (UTC)
← Previous IDNext ID →		

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)