



CVE-2021-39908

Published on: Not Yet Published

Last Modified on: 09/30/2022 12:58:00 PM UTC

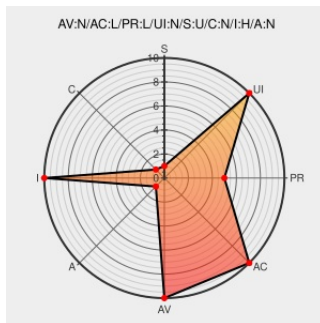
CVE-2021-39908

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

In all versions of GitLab CE/EE starting from 0.8.0 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 certain Unicode characters can be abused to commit malicious code into projects without being noticed in merge request or source code viewer UI.

CVE-2021-39908 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version $\geq 0.8.0$, $< 14.2.6$

Affected Vendor/Software: **GitLab** - **GitLab** version ≥ 14.3 , $< 14.3.4$

Affected Vendor/Software: **GitLab** - **GitLab** version ≥ 14.4 , $< 14.4.1$

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References		
Description	Tags	Link
2021/CVE-2021-39908.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39908.json
HackerOne	hackerone.com text/html	 MISC hackerone.com/reports/1280077
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/337193
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.		

Related QID Numbers
376040 GitLab Multiple Security Vulnerabilities (gitlab release-14.2.6,14.3.4,14.4.1)

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	14.4.0	All	All	All
Application	Gitlab	Gitlab	14.4.0	All	All	All
cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						
cpe:2.3:a:gitlab:gitlab:14.4.0:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:14.4.0:*:*:enterprise:*:*:						

Discovery Credit
Thanks @nickboucher, for reporting this vulnerability through our HackerOne bug bounty program

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-39908 : In all versions of GitLab CE/EE, certain Unicode characters can be abused to commit malicious code... twitter.com/i/web/status/1...	2022-04-01 23:29:34
 @LinInfoSec	Gitlab - CVE-2021-39908: hackerone.com/reports/1280077	2022-04-02 01:01:26
 /r/netcve	CVE-2021-39908	2022-04-02 00:39:03

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)