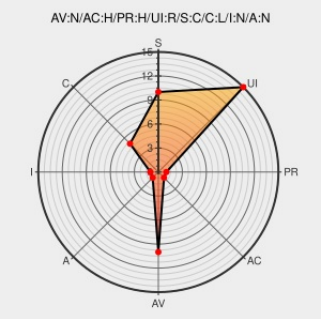
CVE-2022-1157

Published on: Not Yet Published

Last Modified on: 04/18/2022 06:29:00 PM UTC

CVE-2022-1157

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

Missing sanitization of logged exception messages in all versions prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 of GitLab CE/EE causes potential sensitive values in invalid URLs to be logged

CVE-2022-1157 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **<14.7.7**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.8, <14.8.5**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.9, <14.9.2**

CVSS3 Score: 2.4 - LOW

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
2022/CVE-2022-1157.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1157.json
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/37261

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

690828 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (8657eedd-b423-11ec-9559-001b217b3468)

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)
@CVEreport	CVE-2022-1157 : Missing sanitization of logged exception messages in all versions prior to 14.7.7, 14.8 prior to 14… twitter.com/i/web/status/1…	2022-04-11 20:07:52

← Previous ID

Next ID→

© 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 registred 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