



CVE-2018-19585

Published on: 05/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19585

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

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

GitLab CE/EE versions 8.18 up to 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1 have CRLF Injection in Project Mirroring when using the Git protocol.

CVE-2018-19585 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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
Releases GitLab	Release Notes Vendor Advisory about.gitlab.com text/html	MISC about.gitlab.com/blog/categories/releases/

GitLab 11.4.7 Remote Code Execution ~ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

MISC [packetstormsecurity.com/files/160699/GitLab-11.4.7-Remote-Code-Execution.html](#)

GitLab Security Release: 11.5.1, 11.4.8, and 11.3.11 | GitLab

[Release Notes](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

MISC [about.gitlab.com/2018/11/28/security-release-gitlab-11-dot-5-dot-1-released/](#)

GitLab 11.4.7 Remote Code Execution ~ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

MISC [packetstormsecurity.com/files/160516/GitLab-11.4.7-Remote-Code-Execution.html](#)

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

Exploit/POC from Github

Fixed version of the Python script to exploit CVE-2018-19571 and CVE-2018-19585 (GitLab 11.4.7 - Authenticated Remote...

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

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](#)