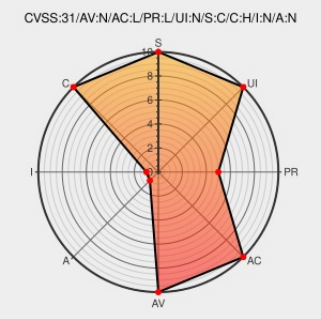
CVE-2018-19571

Published on: 07/10/2019 12:00:00 AM UTC

Last Modified on: 03/01/2023 03:45:00 PM UTC

CVE-2018-19571

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 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an SSRF vulnerability in webhooks.

CVE-2018-19571 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.7 - HIGH

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

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
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 |	Release Notes	MISC about.gitlab.com/2018/11/28/security-

GitLab	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	release-gitlab-11-dot-5-dot-1-released/
SSRF in project integrations (webhook) (#53242) · Issues · GitLab.org / GitLab FOSS · GitLab	Issue Tracking Vendor Advisory gitlab.com text/html	MISC gitlab.com/gitlab-org/gitlab-ce/issues/53242
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

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

← Previous ID

Next ID→

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