

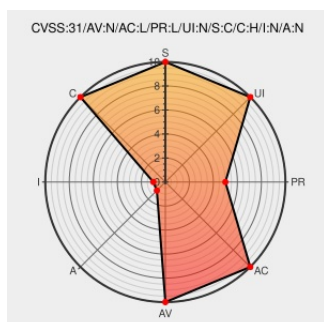


# CVE-2018-19571

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 [M](#) 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    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **4 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

## CVE References

| Description                                          | Tags                                                                 | Link                                                                                                         |
|------------------------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| GitLab 11.4.7 Remote Code Execution ~ Packet Storm   | <a href="#">packetstormsecurity.com</a><br><a href="#">text/html</a> | <b>MISC</b><br><a href="#">packetstormsecurity.com/files/160699/GitLab-11.4.7-Remote-Code-Execution.html</a> |
| GitLab Security Release: 11.5.1, 11.4.8, and 11.3.11 | <a href="#">Release Notes</a>                                        | <b>MISC</b> <a href="#">about.gitlab.com/2018/11/28/security-</a>                                            |

|                                                                                              |                                                                                                                                                               |                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GitLab                                                                                       | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> | <a href="#">release-gitlab-11-dot-5-dot-1-released/</a>                                                                                                                                |
| SSRF in project integrations (webhook) (#53242) · Issues · GitLab.org / GitLab FOSS · GitLab | <a href="#">Issue Tracking</a><br><a href="#">Vendor Advisory</a><br><a href="#">gitlab.com</a><br><a href="#">text/html</a>                                  |  <a href="#">MISC gitlab.com/gitlab-org/gitlab-ce/issues/53242</a>                                  |
| GitLab 11.4.7 Remote Code Execution ~ Packet Storm                                           | <a href="#">packetstormsecurity.com</a><br><a href="#">text/html</a>                                                                                          |  <a href="#">MISC packetstormsecurity.com/files/160516/GitLab-11.4.7-Remote-Code-Execution.html</a> |

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](mailto: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                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | All     | All    | All     | All      |
| Application                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | All     | All    | All     | All      |
| Application                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | All     | All    | All     | All      |
| Application                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | 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 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](#)