



# Webplate is Vulnerable to Authenticated SSRF via Project Backup Import bypassing validate\_repo\_url

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-41654
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 15:16:07 UTC
<b>Updated</b>	2026-05-07 15:46:27 UTC

**Description** Webplate is a web based localization tool. Prior to version 5.17.1, an authenticated user with project.add permission (default

## Risk And Classification

**Primary CVSS:** v4.0 5.3 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000930000 probability, percentile 0.258140000 (date 2026-05-09)

**Problem Types:** CWE-20 | CWE-918 | CWE-20 CWE-20: Improper Input Validation | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/S
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/S

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality	None
Integrity	None
Availability	None
Sub Conf.	Low
Sub Integrity	None
Sub Availability	None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">WeblateOrg</a>	<a href="#">Weblate</a>	affected < 5.17.1	Not specified

#### References

Reference	Source	Link	Tag
<a href="https://github.com/WeblateOrg/weblate/pull/19062">github.com/WeblateOrg/weblate/pull/19062</a>	security-advisories@github.com	<a href="#">github.com</a>	
<a href="https://github.com/WeblateOrg/weblate/security/advisories/GHSA-cwcx-382v-8m9g">github.com/WeblateOrg/weblate/security/advisories/GHSA-cwcx-382v-8m9g</a>	security-advisories@github.com	<a href="#">github.com</a>	
<a href="https://github.com/WeblateOrg/weblate/pull/19061">github.com/WeblateOrg/weblate/pull/19061</a>	security-advisories@github.com	<a href="#">github.com</a>	
<a href="https://github.com/WeblateOrg/weblate/releases/tag/weblate-5.17.1">github.com/WeblateOrg/weblate/releases/tag/weblate-5.17.1</a>	security-advisories@github.com	<a href="#">github.com</a>	
<a href="https://github.com/WeblateOrg/weblate/commit/e4b67a76d95d5165ecb9937f7485fd79223...">github.com/WeblateOrg/weblate/commit/e4b67a76d95d5165ecb9937f7485fd79223...</a>	security-advisories@github.com	<a href="#">github.com</a>	
<a href="https://github.com/WeblateOrg/weblate/commit/e1eff1f517c1ee315d69581910baaabb724...">github.com/WeblateOrg/weblate/commit/e1eff1f517c1ee315d69581910baaabb724...</a>	security-advisories@github.com	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)