



# Thymeleaf: Improper recognition of unauthorized syntax patterns in sandboxed Thymeleaf expressions

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

## Summary

<b>CVE</b>	CVE-2026-41901
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-12 23:16:17 UTC
<b>Updated</b>	2026-05-12 23:16:17 UTC

**Description** Thymeleaf is a server-side Java template engine for web and standalone environments. Prior to 3.1.5.RELEASE, a security

## Risk And Classification

**Primary CVSS:** v3.1 9 CRITICAL from security-advisories@github.com

**CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H**

**Problem Types:** CWE-917 | CWE-1336 | CWE-917 CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') | CWE-1336 CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9	CRITICAL	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9	CRITICAL	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

- Attack Vector: **Network**
- Attack Complexity: **High**
- Privileges Required: **None**
- User Interaction: **None**
- Scope: **Changed**
- Confidentiality: **None**

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Thymeleaf	Thymeleaf	affected < 3.1.5.RELEASE	Not specified

### References

Reference	Source	Link	Tags
github.com/thymeleaf/thymeleaf/security/advisories/GHSA-c9ph-gxww-7744	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

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 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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)